НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра
зі спеціальності 172 Телекомунікації та радіотехніка
на тему: «Дослідження методів забезпечення QoS в мультисервісних IP-мережах»

Виконала:
студентка ІІ курсу, групи ТС-61м
Мєлєхова Марія Олегівна _____

Керівник:
доцент кафедри Телекомунікаційних систем, доцент
Носков Вячеслав Іванович _____

Рецензент:
незалежний експерт за телекомунікацій
к.т.н. Вахрушев Володимир Платонович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2018 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-науковою програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Мєлєховій Марії Олегівні

1. Тема дисертації «Дослідження методів забезпечення QoS в мультисервісних IP-мережах», науковий керівник дисертації Носков Вячеслав Іванович, доцент кафедри Телекомунікаційних систем, доцент, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації _____

3. Об’єкт дослідження TCP/IP мережа.

4. Предмет дослідження методи забезпечення належних якісних показників різноманітних інфо-комунікаційних послуг у TCP/IP мережі.

5. Перелік завдань, які потрібно розробити:

- проаналізувати інфроструктуру сучасної мультисервісної IP-мережі;

- розглянути характеристики різних типів трафіку і їх вимог до якості обслуговування;

- розглянути модель OSI;

- проаналізувати методів підвищення якості обслуговування;

- дослідити якості обслуговування, повіняння методів щодо параметрів середня затримка, бітрейт, джитер, втрата пакетів та вибір певного методу по

параметру затримки для мультисервісної мережі з IP-телефонією- дослідити інструментарій для реалізації алгоритму та представити прототип програмної реалізації алгоритму.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу

Плакат №1 «Тема, мета та завдання магістерської дисертації»

Плакат №2 «Параметри якості передачі трафіку»

Плакат №3. «Методи покращення показників QoS»

Плакат №4. «Математична модель обслуговування трафіку»

Плакат №5. «Результати експерементальних досліджень»

Плакат №6. «Висновки»

7. Перелік публікацій

1. Mieliekhova M. Prioritization of Network Traffic to Improve VoIP Traffic Quality / M. Mieliekhova, O. Starkova, K. Herasymenko. // Third International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2016). – 2016.
2. Мєлєхова М. О. Аналіз алгоритмів регулювання завантаженості IP-мережі../ М.О. Мєлєхова, В.І. Носков, К.В. Герасименко, О.В. Старкова // Одинадцята міжнародна науково-технічна конференція \"Проблеми телекомунікацій\", 2017. – С. 149-152.
3. Мєлєхова М. О. Забезпечення QoS в TCP/IP мережах / М.О. Мєлєхова, В.І. Носков // Дванадцята міжнародна науково-технічна конференція \"Проблеми телекомунікацій\" , 2018. – С. 137-139.

8. Дата видачі завдання 10 вересня 2016 р.

Календарний план

з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
	Пошук джерел інформації та їх систематизація	01.09.2016-01.11.2016	
	Огляд вимог інфо-комунікаційних сервісів до телекомунікаційної мережі	01.11.2016-01.12.2016	
	Аналіз принципів побудови сучасних мультисервісних мереж	01.12.2016-01.01.2017	
	Аналіз методів забезпечення потрібної якості послуг та пов’язаних з ними протоколів у мультисервісній мережі	01.01.2017-01.04.2017	
	Аналіз засобів управлення мережевим трафіком	01.04.2017-01.09.2017	
	Огляд обланднання і програмного забезпечення необхідного для моделювання	01.09.2017 – 31.12.2017	
	Практичні дослідження параметрів якості передачі різного трафіку у мультисервісній мережі у залежності від методу забезпечення QoS	01.01.2018 – 30.04.2018	
	Вступ, висновки та оформлення роботи	01.05.2018 - 20.05.2018	

Студент Мєлєхова М.О..

Науковий керівник дисертації Носков В.І.

РЕФЕРАТ

Обсяг магістерської дисертації складає 102 сторінки, зокрема 52 ілюстрації, 24 таблиці, 6 формул та 31 джерело інформації.

Актуальність теми. У телекомунікаційних мережах є перевантаження, які як правило виникають через зростання числа користувачів послуг зв'язку, збільшенням кількості підкючених до мережі Інтернет пристроїв, збільшенням обсягів трафіку, переходом по зберіганню даних "у хмарі", жорсткістю вимог до якості послуг, що надаються одним з часто виникаючих явищ в сучасних. Під перевантаженням розуміється перевищення вимог споживачів за швидкістю над пропускною здатністю каналу. Тому є важливим при налаштуванні мережі розподілити ресурси, щоб управління було ефективним, насамперед це стосуєтьться мультисервісних мереж в яких передаєтються різні типи трафіку.

Об'єкт дослідження – TCP/IP мережа.

Предмет дослідження – методи забезпечення належних якісних показників різноманітних інфо-комунікаційних послуг у TCP/IP мережі.

Мета та завдання дослідження. Метою роботи є

- Одержання результатів досліджень методів забезпечення належних якісних показників інфо-комунікаційних послуг у мультисервісній TCP/IP мережі.
- Розробка практичних рекомендацій для підвищення якості *IP*-телефонії.

Для досягнення поставленої мети були сформульовані наступні завдання:

1. Проаналізувати інфроструктуру сучасної мультисервісної IP-мережі.

2. Розглянути характеристики різних типів трафіку та їх вимоги до якості обслуговування

3. Проаналізувати методи підвищення якості обслуговування

4. Дослідити методи обслуговування трафіку та порівняти їх щодо наступних параметрів: середня затримка, бітрейт, джитер, втрата пакетів

5. Надати рекомендації щодо вибору методу обслуговування трафіку по параметру затримки пакетів для мультисервісної мережі з IP-телефонією.

Методи дослідження:

1) Створення математичної моделі TCP-сеансів для дослідження параметрів якості передаваємого трафіку;

2) Практичні дослідження парметрів якості передачі трафіку на натурній моделі.

Наукова новизна отриманих результатів:

1) Нові методики і методичні рекомендації які дозволять одержати належні якісні показники інфо-комунікаційних послуг у мультисервісній TCP/IP мережі та розробити практичні рекомендації для підвищення якості IP-телефонії, як найбільш чутливої послуги;

2) Покращення існуючих технологій за рахунок комбінування декількох програмних і апаратних рішень для мультисерсвісної мережі.

Практичне значення отриманих результатів. Рекомендації щодо налаштування мережевих пристроїв згідно з підходами, дослідженими в даній роботі. Покращення ефективності використання фізичних ресурсів існуючої IP-мережі.

Апробація результатів дисертації. Основні результати дисертаційного дослідження оприлюднено в ході 2 наукових конференцій, серед яких:

- Третя міжнародна науково-технічна конференція "Проблеми інфокомунікацій" (PICS&T-2016);
- Одинадцята міжнародна науково-технічна конференція "Проблеми телекомунікацій", 2017 р. (ІТС, НТУУ “КПІ ім. Ігоря Сікорського”);
- Дванадцята міжнародна науково-технічна конференція "Проблеми телекомунікацій", 2018 р. (ІТС, НТУУ “КПІ ім. Ігоря Сікорського”).

Публікації. Основні положення і результати дисертаційної роботи знайшли своє відображення у 3 публікаціях: на Дванадцятій міжнародній науково-технічній конференції "Проблеми телекомунікацій", 2018 р., Одинадцята міжнародна науково-технічна конференція "Проблеми телекомунікацій", 2017 р та на Міжнародній науково-практичній конференції «Проблеми інфокомунікацій », 2016.

Ключові слова: *IP-мережі, QoS, мультисервісний трафік, VoIP, активне управління чергою.*

ABSTRACT

The work contains 102 pages, 52 illustrations, 24 tables, 6 formulas and 31 sources.

Relevance of the topic. Telecommunication networks have congestions, which as a rule arise due to an increase in the number of communication service users, an increase in the number of devices upgraded to the Internet, increased traffic volumes, the transition to the storage of "cloud data", the stringency of requirements to the quality of services provided by one often occurring phenomena in modern. Under overload refers to exceeding the requirements of consumers at speed over channel bandwidth. Therefore, it is important for network configuration to allocate resources so that management is effective, especially for multiservice networks in which different types of traffic are transmitted.

The object of research - TCP / IP network.

The subject of the research is the methods of ensuring the proper quality indicators of various information and communication services in the TCP / IP network.

The purpose and objectives are:

- Obtaining the results of research on the methods of providing adequate quality indicators of information and communication services in the multiservice TCP/IP network.

- Development of practical recommendations for improving the quality of IP-telephony.

To achieve the goal, the following objectives were formulated:

1. To analyze the infostructure of a modern multiservice IP network.

2. Examining the characteristics of different types of traffic and their requirements for quality of service

3. Examining the OSI model

4. Analysis of methods for improving the quality of service.

5. Quality analysis of services, methods of balancing the parameters of the average delay, bitrate, jitter, loss of packets and the choice of a specific method for the delay parameter for multiservice network with IP telephony.

Research methods. To classify the dynamic model of TCP sessions, which is given by a system of nonlinear differential equations. Using the theory of bifurcations, you can

obtain the conditions for the stability of TCP sessions. The method of optimizing TCP sessions for calculating the basic parameters will be investigated.

Scientific novelty of the obtained results.

1) New methodologies and methodological recommendations that will allow: to obtain the results of methods of providing adequate qualitative indicators of information and communication services in the multiservice TCP / IP network and to develop practical recommendations for improving the quality of IP-telephony.

2) Improvement of existing technologies by combining several software and hardware solutions for the multiservice network.

The practical significance of the results. Configure network devices according to the approaches studied in this paper. Improve the efficiency of using the physical resources of the existing IP network.

Approbation of the results of the dissertation. The main results of the dissertation research were published during 2 scientific conferences, among them:

- Third International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2016);
- Elevens International Scientific and Technical Conference "Problems of Telecommunications", 2018 (ITS, NTUU "KPI named after Igor Sikorsky");
- Twelfth International Scientific and Technical Conference "Problems of Telecommunications", 2018 (ITS, NTUU "KPI named after Igor Sikorsky").

Publications. The main positions and results of the dissertation work were reflected in 3 publications: the Twelfth International Scientific and Technical Conference "Problems of Telecommunications", 2018 (ITS, NTUU "KPI named after Igor Sikorsky"), Eleventh International Scientific and Technical Conference "Problems of Telecommunications ", 2017 (ITS, NTUU" KPI named after Igor Sikorsky ") and at the International scientific and practical conference" Problems of infocommunications ", 2016.

Keywords: IP-networks, QoS, multiservice traffic, VoIP, active queue management.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧОК І СКОРОЧЕНЬ

BGP	Border Gateway Protocol, протокол граничного шлюза
CBQ	Модель організації черг з використанням класів
CBWFQ	Class Based Weighted Fair Queueing
CoS	Клас сервісу
CQ	Модель обслуговування, налаштованого користувачем
DNS	Служба домених імен
DSCP	Поле коду диференційованої послуги
ECN	Explicit Congestion Notification
EIGRP	Enhanced Interior Gateway Routing Protocol
ETSI	Європейський інститут стандартизації телекомунікацій
FIFO	Модель перший прийшов - перший на обслуговування
FTP	Протокол передачі файлів
HSRP	Hot Standby Router Protocol,
HTTP	Протокол передачі гіпертексту
IETF	Відкрите міжнародне співтовариство проектувальників
IP	Інтернет протокол
ITU-T	Міжнародний союз телекомунікацій
LAN	Local Area Network
LLQ	Low-latency queuing
MPLS	Багатопротокольна комутація на основі міток
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit

NGN	Мережа наступного покоління
OSI	Модель взаємодії відкритих систем
PQ	Модель пріорітетного обслуговування
QoS	Якість обслуговування, якість надання послуг, якість сервісу
RED	Random Early Detection
RFC	Request for Comments - рекомендації
RIP	Routing Information Protocol, протокол маршрутизації
RSVP	Протокол резервування ресурсів
SMTP	Простий протокол пересилання пошти
TCP/IP	Мережева модель передачі даних
ToS	Рівень пріоритету IP, вид послуги
VLAN	Віртуальна локальна мережа
VoIP	Телефонія на основі протоколу IP
WFQ	Зважене справедливе обслуговування
WRED	Weighted RED
ПЗ	Програмне забезпечення
ПК	Персональний комп'ютер
ТКС	Телекомунікаційна система
ТМЗК	Телефонна мережа загального користування

ВСТУП

Розвиток сучасних мультисервісних комп’ютерних мереж – є важливим питанням сучасного суспільства: по-перше, мультисервісні комп’ютерні мережі є необхідним фактором для доступу людини до сучасних технологій, які значно полегшують життя, по-друге, розвиток мультисервісних мереж є важливою складовою розвитку економіки як на рівні окремого підприємства, так і державному рівні .

Упраління чергами у мережі дозволає мережі моніторити себе і підлаштовуватись під зміни в залежності від навантаження на мережу. Наприклад, шейпінг догволяє забезпечити "плавність" передачі даних, деякий час тримаючи пакети в буфері, що є перевагою особливо при передачі голосового трафіку, а полісінг дозволяє відкидати пакети, аби при передачі не утворився затор. За допомогою цих механізмів використання мережевих ресурсів є більш ефективним, а можливість утворення заторів є меншою.

IP-телефонія займає особливе місце в сучасних мультисервісних мережах. Впровадження *IP*-телефонії потребує строгого дотримання вимог до інфраструктури в якій вона впроваджується, які будуть далі розглянуті.

РОЗДІЛ 1. АНАЛІЗ ПЕРЕДАЧІ МУЛЬТИСЕРВІСНОГО ТРАФІКУ ПО IP-МЕРЕЖАМ

1.1 Характеристика сучасних мультисервісних мереж

У зв’язку зі зростанням числа користувачів послуг зв’язку, збільшенням кількості підкючених до мережі Інтернет пристроїв, збільшенням обсягів трафіку, переходом по зберіганню даних "у хмарі", жорсткістю вимог до якості послуг, що надаються одним з часто виникаючих явищ в сучасних телекомунікаційних мережах є перевантаження (congestion). При цьому під перевантаженням розуміється перевищення вимог споживачів за швидкістю над пропускною здатністю каналу. Тому досить важливо при налаштуванні мережі розподілити ресурси, щоб управління було ефективним, насамперед це стосуєтьться мультисервісних мереж в яких передаєтються різні типи трафіку.[1]

Мультисервісна мережа - це мережа по якій передаються голос, відео, дані. Наприклад, якщо раніше телефоний звязок і доступ до Інтернету в офісі разгорталися окремо, то зараз у більшості офісів разгортається єдина мережа для передачі різних типів даних. Основною перевагою даного рішення є зменшення витрат по розгортанню інфраструктури.

Основне завдання мультисервісних мереж - забезпечення роботи різнорідних інформаційних і телекомунікаційних систем і додатків в єдиному транспортному середовищі, тобто коли для передачі і звичайних даних, і голосу, відео та ін. використовується єдина інфраструктура.

Різні види інформації мультимедійної мережі вимагають підтримки відповідних механізмів забезпечення якості обслуговування QoS. Термін якість обслуговування загалом описує вимоги додатку до роботи мережвої служби. Кожен тип додатку може бути проаналізований по відношенню до вимог QoS, які він пред'являє службам до мережі. Якщо ці вимоги будуть дотримані, то додаток буде ефектифно працювати.

Стандартні IP-мережі не гарантують ніякого показника QoS. Якщо взяти за основу ATM, що забезпечує передачу необхідного QoS будь-якої мультимедійного трафіку, то реалізація виявиться практично неможливою для мереж загального користування через великі витрати. [2]

Таким чином, з'явилася необхідність забезпечити підтримку різного роду мультимедійного трафіку з різноманітними вимогами до рівня QoS в рамках архітектури IP-мережі.

1.2 Інфроструктура IP-мережі

В загалом IP-мережі базуються на клієнт-серверній архітектурі, яка визначає лише загальні принципи взаємодії між комп'ютерами, деталі взаємодії визначають різні протоколи. Дана концепція нам говорить, що потрібно розділити машини в мережі на клієнтські, яким завжди щось потрібно і на серверні, які дають те, що потрібно. При цьому взаємодія завжди починає клієнт, а правила, за якими відбувається взаємодія, описує протокол. Дані зберігаються на потужному комп'ютері - сервері. Досить часто сервер розташовується в окремому приміщенні і обслуговується системним адміністратором. Комп'ютери-клієнти зазвичай є менш потужними і мають віддалений доступ до інформації та програм, що зберігаються на сервері. Клієнтська і серверна машини об'єднані в мережу, як показано на рис. 1.1. Мережа, через яку дані передаються від однієї машини до іншої, позначена на рисунку хмарою. [3]

Дана система називається клієнт-серверною моделлю. Вона в основному є основою побудови всієї мережі. Найпопулярніша реалізація - веб-додаток, в якому сервер генерує веб-сторінки, засновані на його базі даних у відповідь на запити клієнта, які можуть оновити базу даних. Вона може бути застосована, коли клієнт і сервер знаходяться в одній будівлі і належать одній компанії, а також коли вони розташовані далеко один від одного. Наприклад, коли користувач отримує доступ до інтернет-сайту, працює та ж модель. При цьому веб-сервер грає роль серверної машини, а комп'ютер користувача - клієнтської.[3]

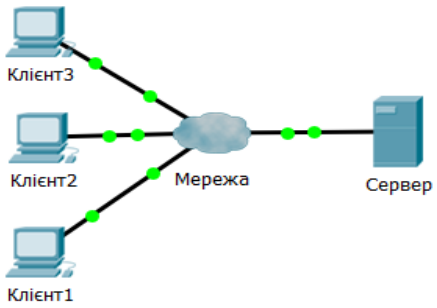


Рисунок 1.1 Архітектура клієнт-сервер

В роботі мережі можна завжди виділити два процеси: серверні і клієнтські. Найчастіше обмін інформацією відбувається так: клієнт надсилає запит серверу через мережу і чекає на відповідь; при прийнятті запиту сервер виконує певний алгоритм дій або шукає запитувані дані і відсилає відповідь.

Інфраструктура мережі складається з трьох основних компонент[4]:

- пристрої;
- середа передачі даних;
- сервіси.

Пристрої можуть бути мережеві та кінцеві. До кінцевих пристроїв належать:

- комп'ютери (робочі станції, ноутбуки, файлові сервери, веб-сервери);
- термінальне устаткування TelePresence;
- камери відеоспостереження;
- VoIP-телефони;
- мобільні старт-пристрої (смартфони, планшетні ПК, смарт-годинники);
- мережеві принтери.

Мережеві пристрої[4]:

Модеми. Існує три основних типи модемів. Модеми перетворюють цифрові дані комп'ютера у формат, який може передаватися в мережі провайдера. Аналоговий модем перетворює цифрові дані на аналогові сигнали для передачі через аналогові телефонні лінії. Модем цифрової абонентської лінії (DSL) з'єднує мережу користувача безпосередньо з цифровою інфраструктурою телефонної

компанії. Кабельний модем підключає мережу користувача до постачальника кабельних послуг, який зазвичай використовує гібридну коаксіальну (HFC) мережу.

Концентратори. Концентратори отримують дані на один порт, а потім надсилають їм на всі всі інші порти. Ці пристрої розширюють доступ до мережі, оскільки вони відновлюють електричний сигнал. Вони також можуть підключатися до іншого мережевого пристрою, наприклад, комутатора або маршрутизатора, який підключається до інших сегментів мережі.

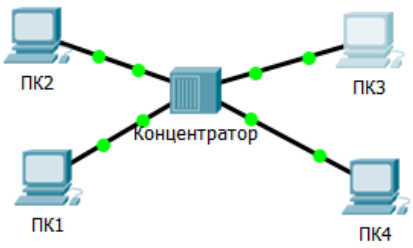


Рисунок 1.2. Схема мережі з підключеним концентратором

Мости. Щоб розділити мережі на сегменти були введені мости. Вони записують всі пристрої на кожному сегменті мережі. Міст може фільтрувати мережевий трафік між мережевими сегментами, що допомагає зменшити обсяг трафіку між пристроями.

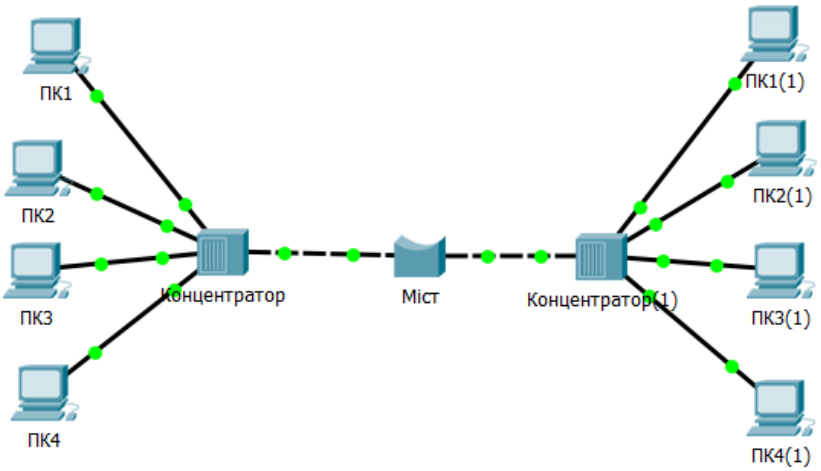


Рисунок 1.3 Схема мережі з підключеним мостом

Комутатори (L2). Дані пристрої, на відміну від концентраторів і мостів, мікросегментують локальну мережу, що означає - трафік надсилається тільки до тих пристроїв, яким він адресований. Це забезпечує високу роздільну пропускну здатність для кожного пристрою в мережі. Якщо на комунікаторі до кожного порту встановлено лише одне пристрій, він працює в режимі повного дуплексу. Комутатори підтримують таблицю комутації, яка містить список усіх MAC-адрес у мережі, а список яких порту комутатора можна використовувати для досягнення пристрою з заданою MAC-адресою.

Таблиця комутації записує MAC-адреси, перевіряючи MAC-адресу відправника кожного вхідного фрейму, а також порт, на якому надходить фрейм. Після цього пристрій створює таблицю комутації, яка відображає MAC-адреси для вихідних портів. Коли трафік надходить, призначений для певної MAC-адреси, комутатор використовує таблицю, щоб визначити, який порт він використовуватиме для досягнення MAC-адреси. Трафік передається від порту до пункту призначення. Відправляючи трафік лише з одного порту до пункту призначення, інші порти не зазнають впливу.

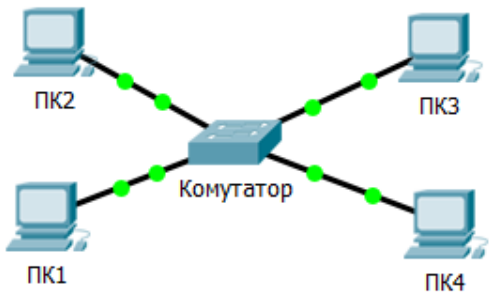


Рисунок 1.4 Схема мережі з підключеним комутатором

Безпроводові точки доступу, показані на рисунку 1, забезпечують доступ до мережі для безпроводових пристроїв, таких як ноутбуки та планшети. Точка безпроводового доступу використовує радіохвилі для зв'язку з кінцевими пристроями або іншими точками доступу. Вона має обмежений діапазон покриття. Великі мережі вимагають декількох точок доступу для забезпечення покриття.

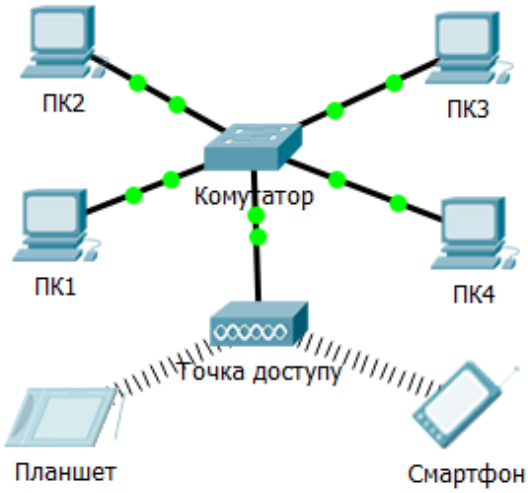


Рисунок 1.5 Схема мережі з підключеною точкою доступу

Маршрутизатори підключають мережі, як показано на малюнку 2. Маршрутизатори використовують IP-адреси для пересилання трафіку в інші мережі. Маршрутизатор служить шлюзом для зовнішніх мереж.

Рисунок 1.6 Схема мережі з підключеним маршрутизатором та виходом у WAN-мережу

Деякі пристрої можуть містити в собі декілька з вище описаних функцій, наприклад багатофункціональний пристрій або беспровідний маршрутизатор. Він включає в себе маршрутазатор(WAN-порт), комутатор(LAN-порти) і точку безпроводового доступу. Для деяких мереж зручніше придбати та налаштувати один пристрій, ніж придбання окремого пристрою для кожної функції. Це особливо зручно для домашнього або малого офісу. Багатофункціональні пристрої можуть також включати модем.

До основних функцій мережевих пристроїв відноситься управління даними в процесі їх проходження через мережу. Ці пристрої використовують адресу вузла призначення у поєднанні з інформацією про зв'язки в мережі, щоб визначити шляхи для відправки повідомлень по мережі.

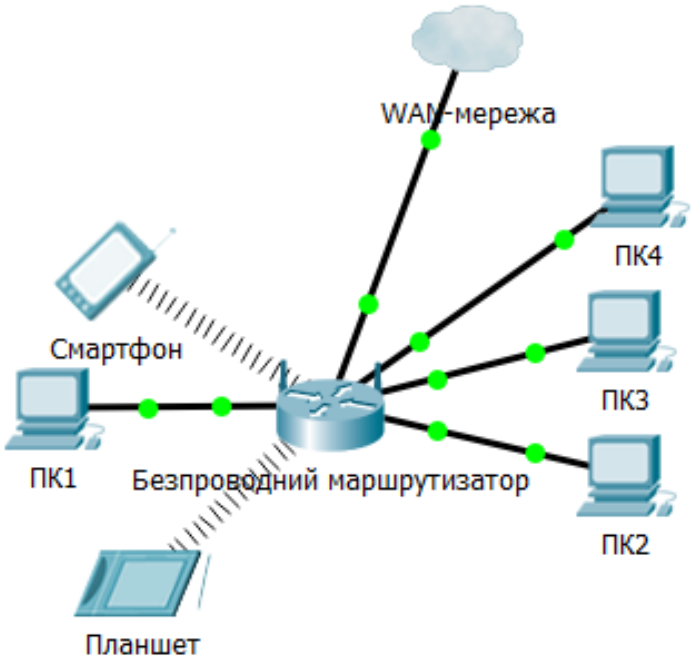


Рисунок 1.6 Схема мережі SOHO (Small Home Small OffiCe) з беспроводним маршрутизатором

Процеси, запущені на проміжних мережевих пристроях, виконують наступні функції:

- регенерація і ретрансляція сигналів передачі даних;
- пошук оптимальних маршрутів;
- інформування інших пристроїв про колізії та збої;
- переключення передачі даних через альтернативний маршрут при виході каналу з ладу;
- класифікація і передача повідомлень відповідно до пріоритетів якості обслуговування (QoS);
- дозвіл або заборона потоку даних на підставі налаштувань безпеки.

Для проектування мережі, потрібно правильно підібрати середовище, через яке будуть передаватися дані. Кожне рішення може має свої переваги і недоліки. В ідеальному варіанті оптоволоконний кабель підключається безпосередньо до мережі малих і домашніх офісів. У деяких місцях розташування підтримується тільки один спосіб підключення. Тому необхідно провести аналіз співвідношення витрат і переваг для визначення рішення. Існують це проводові та безпроводові способи передачі даних.[5]

До провідних відносятся - вита пара, коаксіальний кабель, оптоволокно. У витій парі, як і у коаксіальних кабелях, для передачі даних використовуються електричні сигнали. В оптоволоконних кабелях для передачі даних використовуються світлові сигнали. Ці кабелі розрізняються пропускною спроможністю, розміром і вартістю.

Вита пара - це тип мідного кабелю, який використовується для телефонного зв'язку та більшості мереж Ethernet. Вита пара забезпечує захист від взаємних або перехресних наведень, тобто від шуму, створюваного сусідніми парами проводів в кабелі.

Коаксіальний кабель зазвичай виготовлений з міді або алюмінію. Він використовується в кабельному телебаченні і в системах супутникового зв'язку. По коаксіальному кабелю проходять дані в формі електричних сигналів. Екранування у нього краще, ніж у неекранованої кручений пари (UTP), відношення сигнал/шум вище. Однак вита пара замінила коаксіальний кабель в локальних мережах, оскільки

в порівнянні з неекранованої кручений парою коаксіальний кабель складніше в прокладенні, дорожчий і гірше піддається ремонту.

В оптоволоконих кабелях для передачі сигналів використовується світло і такий кабель не схильний до впливу електромагнітних або РЧ-завад. При вході в кабель всі сигнали перетворюються в світлові імпульси, а при виході з кабелю вони перетворяться назад в електричні сигнали. Оптоволоконний кабель може передавати більш чіткі сигнали, на більшу відстань і з більшою пропускною здатністю, ніж кабель, виготовлений з міді або інших металів. Хоча оптоволокно дуже тонке і гнучке, завдяки властивостям сердечника і оболонки воно дуже міцне. Завдяки своїй міцності оптичне волокно може використовуватися в найважчих умовах експлуатації[5].

До безпроводовим відносяться - радіоканали наземного і супутникового зв'язку

Основні критерії вибору мережевого середовища для організації мережі:

- відстань, на якій фізичне середовище здатне передати сигнал;
- умови установки середовища передачі даних;
- об'єм даних і швидкість передачі фізичного середовища;
- вартість засобів передачі даних і їх установки.

1.3 Особливості передачі мультисервісного трафіку в IP мережах

Для надання користувача сервісів використовується мережеве обраднання. Зазвичай мережевий сервіс надає дані у відповідь на запит. Сервіси люди використовують щодня, наприклад, сервіси електронної пошти і сервіси веб-хостінгу для веб-сайтів. Процеси забезпечують функціональність, яка направляє та транспортує дані по мережі, і вони важливі для роботи мереж.

Інтерактивні мультисервісні мережі надають абонентам широкий спектр послуг : інтернет-телефонію, пакети аналогового і цифрового телебачення,

дистанційне навчання, голосування і опитування населення, відеотелефонію, відео на вимогу, медичні консультації, оплату комунальних послуг.

Основні фактори, які впливають на QoS IP-мережі[4]:

- максимальна пропускна здатність, Мбіт/с - максимальна кількість даних, яку можна передати за одиницю часу;
- затримка, мс - проміжок часу, необхідний для передачі пакета через мережу;
- джиттер, мс - затримка між двома послідовними пакетами;
- втрата пакета, % - відношення кількості пакетів або даних, які були втрачені при передачі через мережу, до загальної кількості переданих даних.

Однак для різних типів трафіку при передачі різні параметри до яких вони чутливі. Напраклад, голос дуже чутливий до затримок. Тому проектуючи мультисервісну мережу необхідно продумати також про які сервіси будуть впроваджені і які вимоги до якості обслуговування. Вимоги до різних типів трафіку суттєво відрізняються. Зазвичай дані не чутливі до невеликих затримок, а дуже важливим при передачі саме достовірність. В залежності від того чи є додатки інтерактивними і наскільки є критичними - можна задати пріорітет.

Голосовий трафік є помірним і стабільним, він не потребує таких ревурсів як відео-трафік. Даний тип є чутливим до затримок і не передається повторно при втраті пакетів, тому зазвичай йому призначають пріорітет. Затримки відповідно до рекомендації ITU-T G.114 і стандартами ETSI ETR 250 і ETR 275 розділені на 4 класи[6]:

- малі (10 ... 15 мс), що не дратують користувачів і не потребують в зв'язку з цим придушення акустичного та електричного ехосигнала;
- невеликі (до 150 мс), що вимагають придушення відлуння, але не впливають критично на взаємодію користувачів;
- допустимі (від 200 до 400 мс), при яких якість взаємодії хоча і погіршується, але може бути прийнятним;

- неприпустимі (більше 400 мс), при яких інтерактивне голосове взаємодія утруднено і необхідне введення деяких правил розмови (наприклад, як в портативних дуплексних радіостанціях - walkie-talkie).

Табл. 1.1 Приклади послуг, що надаються по мультисевісній IP-мережі, та їх показників якості.

Послуги	Вид послуги	Показники качества
Голосові послуги	- Інтернет-телефонія - Відеоконференція - Відеотелефонія - Інтерактивні ігри	Затримка Джиттер Втрати пакетів
	- Покупки в Інтернеті	Втрати пакетів
Послуги передачі повідомлень	- Голосова пошта - Інтернет-факс - Відео пошта - Групова пошта	Відсутні
Послуги передачі даних	- Перегляд Web-сторінок - Загрузка файлів	Відсутні
	- Відео-по-запиту	Втрати пакетів та джитер
Послуги трансляції без індивідуального контролю змісту	- Електронна кореспонденція - Реклама в Інтернеті	Відсутні
	- Трансляція в режимі реального часу	Втрати пакетів
Послуги трансляції з індивідуальним контролем змісту	- “Новини-по-запиту” - “Відео-по-запиту”	Втрати пакетів та джитер

Для голосового трафіку джиттер не повинен перевищувати 30 мс, а втрата пакетів - 1%. Смуга пропускання для голосового трафіку потрібна не менше 30 кбіт/с. Відеотрафік є непомірним і нестабільним, а також має пульсуючий характер. Він, також як і голосовий трафік, чутливий до затримок і джитеру, але в меншій мірі. Його затримка не повинна перевищувати 400 мс, а джиттер - 50 мс. Втрата пакетів повинна бути до 1%. Мінімальна смуга пропускання становить 384 кбіт/с, так як для відеотрафіку необхідно більше ресурсів для передачі, порівняно з даними та голосовим трафіком.

1.4 Еталона модель OSI та модель TCP/IP

Одними з поширених архітектурних типів взаємодії в мережі - еталона модель OSI та TCP/IP.

OSI - це семирівнева модель взаємодії вікритих мереж. Ця модель заснована на розробці Міжнародної організації зі стандартизації (International Organization for Standardization, ISO) і є першим кроком до міжнародної стандартизації протоколів, використовуваних на різних рівнях[4].

Модель TCP/IP була створена дослідниками Міністерства оборони США. Вона складається з рівнів, що виконують необхідні функції з підготовки даних для передачі по мережі. На рис. 1 показані чотири рівні моделі TCP/IP[4].

Назва моделі TCP/IP містить назви двох принципових протоколів транспортного рівня - TCP (протокол управління передачею) і IP (протокол міжмережевого обміну). Протокол TCP відповідає за надійну доставку пакетів.

Протокол IP забезпечує додавання адрес джерела і призначення до даних. Однак модель TCP/IP включає в себе безліч інших протоколів, крім TCP і IP. Ці протоколи утворюють провідний стандарт передачі даних по мережах і через Інтернет.

Модель TCP/IP використовується спеціально для набору протоколів TCP/IP, а модель OSI - для розробки стандартів зв'язку для обладнання і додатків різних постачальників.

Загалом модель TCP/IP виконує ту ж процедуру, що і модель OSI, але використовує чотири рівні замість семи. На рисунку 1.7 показано порівняння рівнів двох моделей[4].

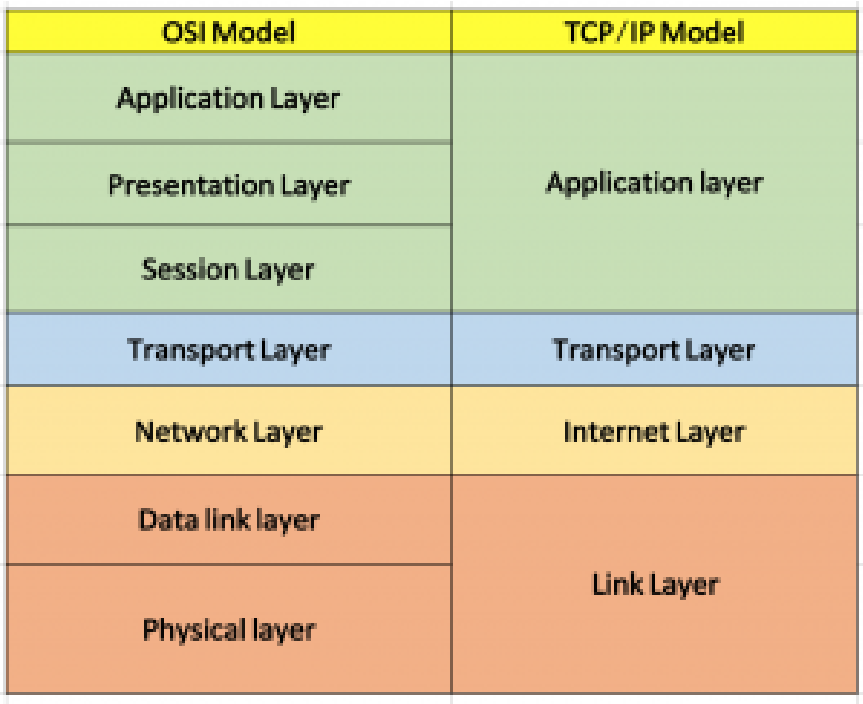


Рисунок 1.7 Порівняння моделей OSI та TCP/IP

Нижче описані рівні та їх характренистики моделі OSI починаючи з фізичного рівня.

1) Фізичний рівень.

Задачею першого рівня є передача бітів по каналу зв'язку. При проектуванні мережі необхідно переконатися, щоб дані передавачися достовірне, тобто при передачі одиниці на приймаючій стороні також повинна бути отримана одиниця, а не нуль.

На данномі рівні приймається до уваги: яка напруга відповідати одиниці, а яка для нуля; яка тривалість біту; який тип передачі по напрямках(симплексна, напівдуплексна чи дуплексна передача); як встановлюється початковий зв'язок і як він припиняється, коли обидві сторони виконали свої завдання; який тип кабелю і які його фізичні характеристики. Питання проектування в основному пов'язане з

механічними, електричними і процедурними інтерфейсами, а також з фізичним носієм, лежачим нижче фізичного рівня.

Вимоги до якості обслуговування на фізичному рівні залежать від вибранного сердедовища для організації мережі.

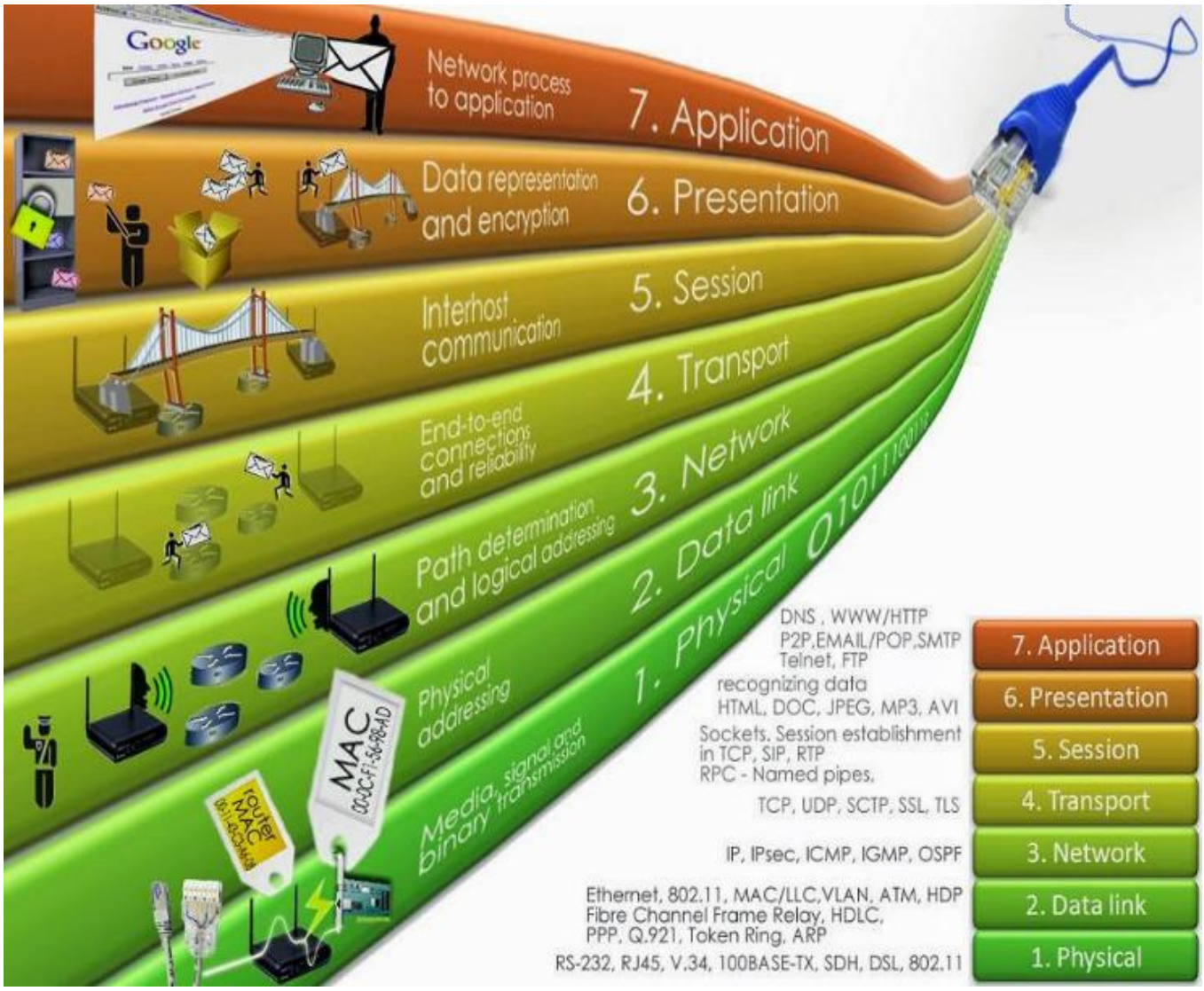


Рисунок 1.8 Модель OSI [9]

2) Канальний рівень.

Основне завдання - установлення, підтримка та розрив зв'язку, бути здатним передавати дані фізичного рівня по надійній лінії зв'язку, вільної від невиявлених помилок, і маскувати реальні помилки, так що мережевий рівень їх не бачить. Це

завдання виконується за допомогою розбиття вхідних даних на кадри(або фрейми), звичайний розмір яких коливається від кількох сотень до кількох тисяч байт. Кадри даних передаються послідовно з обробкою кадрів підтвердження, які надсилаються назад одержувачем. Ще одна проблема, що виникає на рівні передачі даних (а також і на більшій частині більш високих рівнів), - як не допустити ситуації, коли швидкий передавач завалює приймач даними. Може бути передбачений певний механізм регуляції, який інформував би передавач про наявність вільного місця в буфері приймача на поточний момент[13].

Одне з завдань канального рівня - фізична або MAC-адресація. MAC-адреса - фізична адреса пристроя, якою керуються пристрої для передачі карів, складається з 48біт і має вигляд XX-XX-XX-XX-XX-XX, де X - 16-річне число. На відміну від логічної адреси рівня вище, MAC-адреса "вшита" в мережеву плату і її не змінюють. Сфема фрейму Ethernet 802.1Q/P представлена нижче на рисунку 1.9[4].

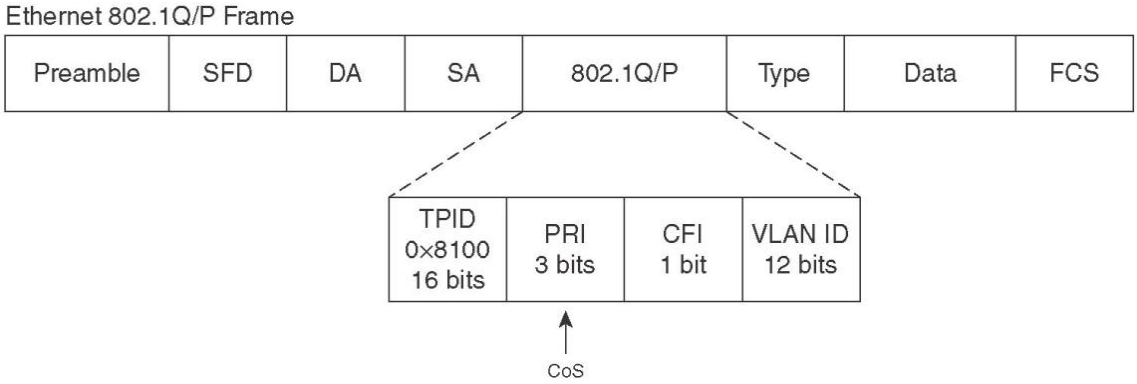


Рисунок 1.9 Схема фрейму Ethernet 802.1Q/P

На канальному рівні можливе маркування кадрів для забезпечення QoS - це клас обслуговування (COS). COS - поле в 3 біта, що дозволяє маркирувати ваш трафік 8-ми різними способами.

3) Мережевий рівень.

Займається визначенням маршрутів пересилки пакетів від передавача до пункту призначення. Маршрутизація - це процес пошуку оптимального маршруту, в залежності від того який протокол маршрутизації налаштований на пристрої.

Маршрутизація може бути як статичною, так і динимічною. Статична маршрутизація - коли маршрути жорстко задані, тобто вручну прописані на пристроях. Динамічна маршрутизація використовує протоколи маршрутизації, які прораховують оптимальний маршрут.

Оптимальним маршрут може бути по певним критеріям, так як напростійший Routing Information Protocol (RIP) використовує лиш кількість переходів, що не є ефективним по декільком причинам, в RIP не враховується:

- пропускна здатність каналів;
- затримки;
- надійність маршруту;
- завантаженість каналів;
- відсутнє балансування навантаження.

Тому RIP і не використровується у досить великих мережах. У протоколі Open Short Path First (OSPF) вже використовується вибір маршруту на основі стану каналу і вже враховується пропускна здатність. EIGRP використовує для розрахунку пріоритетного шляху в своїй метриці - пропоскну здатність, затримки, надійність, завантаженість, а також є можливість налаштувати балансування навантаження для маршрутів з рівними чи різними метриками. Однак чим "розумніший" протокол налаштувати, тип більше обчилувальних ресурсів і памяті небхідно мережевому пристрою, а тому і дорожче мережеве обладнання.

На мережевому рівні інтерфейсам призначаються IP-адреса, яка є ієрархічною, логічною, унікальною адресою. Ієрархічність - так як кожна адреса належить певній LAN з адресою мережі і маскою, яка дану мережу обмежує. Логічність - так як адресу видають на основі місце розташування (в якій LAN) знаходиться пристрій. Унікальною - в мережі не повинно бути дві ідентичні IP-адреси, інакше буде "конфлікт IP-адрес" і дані не будуть передаватися до пристрою з неунікальним ідентифікатором. Існують протоколи IP-адресації версії 4 (IPv4) та версії 6 (IPv6).

Якщо в підмережі одночасно присутня дуже велика кількість пакетів, то можуть утворитися перевантаження у вузьких місцях. Недопущення подібного

також є завданням мережевого рівня в поєднанні з більш високими рівнями, які адаптують навантаження.

Для забезпечення QoS на мережевому рівні використовують маркування IP Precedence (IPP) - значення, що використовує перші 3 біта поля Type of Service (ToS) в заголовку пакета, що дозволяє встановити одне зі значень від 0 до 7, де 0 найменш важливий трафік, а 7 найбільш важливий. Значення 6 і 7 зарезервовані і призначені для протоколів маршрутизації і сигналізації (таких на BFD). Дані в IPP можуть бути завантажені з поля CoS.(табл 1.2)

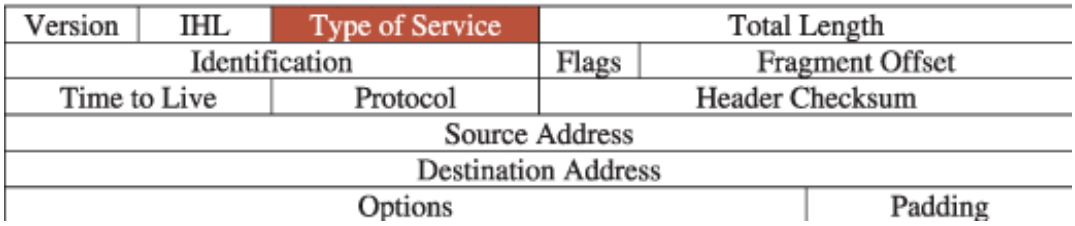


Рисунок 1.10 Заголовок IP-пакету [10]

Таблиця 1.2 Пріорітет полів ToS для мережевих додатків [4]

Precedence	data type	Protocol/application example
0 – routine	Low–priority data	web, bittorrent
1 – зriority	Medium–priority data	SQL, AD
2 – immediate	High-priority data	Citrix ICA, Salesforce
3 – flash	Call Signnaling	RTCP
4 – flash-override	Videoconferencing	WebEx, GoToMeeting
5 – critical	Voice	RTP
6 – internet control	Reserved	
7 – network control	Reserved	

4) Транспортний рівень. Основна функція транспортного рівня - прийняти дані від сеансового рівня, розбити їх при необхідності на невеликі частини, передати їх мережевого рівня і гарантувати, що ці частини в правильному вигляді прибудуть за призначенням. Транспортний рівень також визначає тип сервісу за допомогою

логічного порту, що надається сеансовому рівню і, в кінцевому рахунку, користувачам мережі. В данному випадку порт ідентифікує дані протоколу вищого рівня (додатку), які передаються[13].

Протоколи транспортного рівня:

- Протокол керування передачею, TCP (Transmission Control Protocol)

TCP розбиває конкретний потік даних на порції, та додає до кожної з них заголовок з номером послідовності. Отримані таким чином порції даних традиційно називаються TCP-сегментами. Далі кожний сегмент інкапсулюється в IP-пакет і передається через IP-протокол до хоста-отримувача.

При прередачі по TCP використовується тристороннє рукостискання, яке представлено на рис. 1.11.

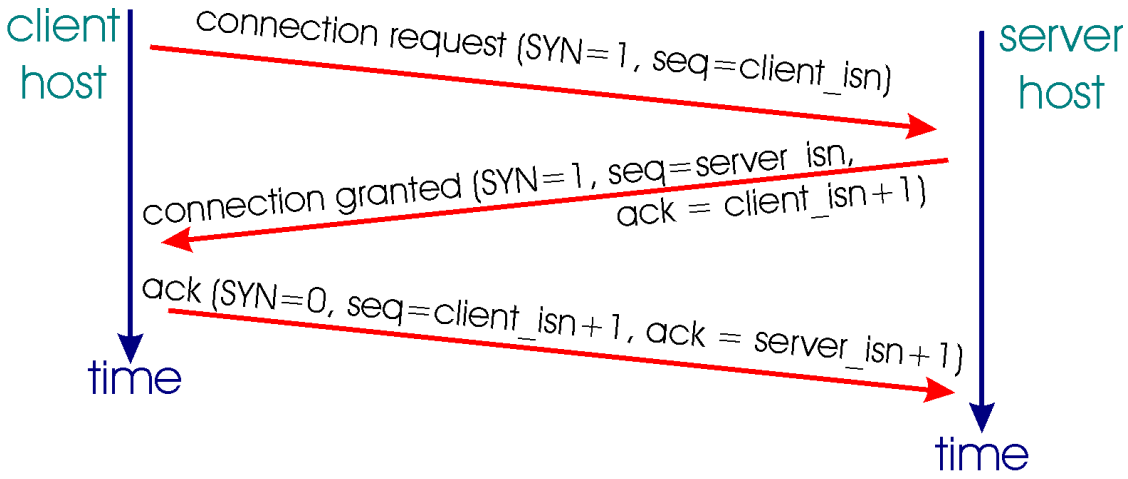


Рисунок 1.11 Тристороннє рукостискання в TCP [11]

Після надходження IP-пакету до хоста-отримувача перевіряється коректність отриманих даних у TCP-сегменті, методом перерахування контрольної суми, та переконується, що попередні сегменти даних також були успішно отримані. Після чого хост-отримувач надсилає запит до хоста-відправника про нову, або повторну передачу порції даних, що одночасно є підтвердженням того, що всі сегменти з номерами послідовності, меншими ніж номер нового запиту, були успішно отримані.

У свою чергу TCP-сегменти деінкапсулюються з IP-пакетів, розміщуються в правильному порядку та з них вилучаються TCP-заголовки. Отриманий таким чином потік даних передається до того протоколу верхнього рівня, з якого первісно надійшли дані на стороні хоста-відправника.

- Протокол призначених для користувача дейтаграм, UDP (User Datagram Protocol), виконує обмін датаграмами без підтвердження та гарантії доставки. При використанні протоколу UDP відповідальність за обробку помилок і повторну передачу даних покладена на протокол рівнем вище. Але попри всі недоліки, протокол UDP є ефективним для серверів, таких таких як передача відео в реальному часі, так як він використовує менше ресурсів.

Використання певного протоколу на транспортному рівні також грає важливу роль у забеченні якості обслуговування.

5) Сеансовий рівень. Дозволяє користувачам різних комп'ютерів встановлювати сеанси зв'язку один з одним. При цьому надаються різні типи сервісів, серед яких управління діалогом (відстеження черговості передачі даних), управління маркерами (запобігання одночасного виконання критичною операції декількома системами) і синхронізація (установка службових міток всередині довгих повідомлень, що дозволяють продовжити передачу з того місця, на якому вона обірвалася , навіть після збою і відновлення)[13].

6) Рівень відображення. На відміну від більш низьких рівнів, завдання яких - достовірна передача бітів і байтів, даний рівень займається здебільшого синтаксисом і семантикою переданої інформації. Щоб було можливо спілкування комп'ютерів з різними внутрішніми уявленнями даних, необхідно перетворювати формати даних один в одного, передаючи їх по мережі в якомусь стандартизований вигляді. Рівень представлення займається цими перетвореннями, надаючи можливість визначення і зміни структур даних більш високого рівня (наприклад, записів баз даних)[13].

7) Прикладний рівень. На даному рівні забезпечується взаємодія додатків конистувачів або між клієнтом і сервером, взаємодія між додатками, використовуваними для обміну даними, і базової мережею, по якій передаються

повідомлення. Протоколи рівня додатків використовуються для обміну даними між програмами, що виконуються на вузлі-джерелі і вузлі-одержувачі. Існує безліч протоколів програм, і постійно розробляються нові протоколи[13].

До деяких з найбільш відомих протоколів програм відносяться: протокол передачі гіпертексту (HTTP), протокол передачі файлів (FTP), простий протокол передачі файлів (TFTP), протокол доступу до повідомлень в Інтернеті (IMAP) і протокол служби доменних імен (DNS).

Протокол передачі гіпертексту HTTP (HyperText Transfer Protocol), який становить основу глобальної мережі Інтернет. Коли браузер запитує веб-сторінку, він передає її ім'я (адресу) і розраховує на те, що сервер, на якому розташована сторінка, буде використовувати HTTP. Сервер у відповідь відсилає сторінку.

Простий протокол пересилання пошти SMTP (SimPle Mail Transfer Protocol) — це протокол, який використовується для пересилання електронної пошти до поштового сервера або з клієнта-комп'ютера, або між поштовими серверами.

Протокол передачі файлів FTP (File Transfer Protocol) — дає можливість користувачу обмінюватися файлами з будь-яким комп'ютером мережі, де підтримується протокол FTP. Для передачі устновлюється два з'єднання - для управління і для передачі даних.

Протокол передачі в режимі реального часу RTP (Real-time TransPort Protocol) - використовується при передачі аудіо і відео даних через IP мережі в режимі реального часу.

Система домених імен DNS (Domain Name System) — ієрархічна розподілена система перетворення імені хоста в IP-адресу.

Протокол динамічної конфігурації вузла DHCP (DynamiC Host Configuration Protocol) - це стандартний протокол рівня додатків, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі.

1.5 Технологія Voice over IP в розрізі моделі OSI

На сьогодні IP-телефонія витісняє традиційні телефонні мережі з комутацією каналів за низької вартісті дзвінків, рахунок легкості розгортання, простоти конфігурації, досить високої якості зв'язку та відносній безпеці з'єднання.

При здійсненні дзвінка сигнал перетворюється в стислий пакет даних. Потім відбувається пересилка даних пакетів по мережі з комутацією пакетів - IP мережі. При досягненні пакетів отримувача, вони декодуються в вид для сприйняття голосових сигналів. Дані процеси проходять за допомогою допоміжних протоколів, деякі з яких будуть розглянуті далі.

В даному розумінні, протокол передачі даних - певна мова, що дозволяє двом абонентам розуміти один одного та забезпечити якісну.

У традиційної телефонії - мережі з комутацією каналів, встановлення з'єднання відбувається через телефоннустанцію. Дані мережі орієнтовні тільки на передачу голосового трафіку. Голосові сигнали проходять по телефонним лінім по виділеному включенню.

У IP-телефонії стислі пакети даних поступають в локальну або глобальну мережу з певною адресою та передаються на основі IP-адреси. Дане рішення є дешевшим як для абонента, так і для оператора завдяки тому, що традиційні телефонні мережі не досить раціонально використовують пропускну здатність каналу, тоді як IP-телефонія використовує стиснення пакетів даних і дозволяє використовувати фізичні ресурси середовища передічі більш ефективно.

На сьогодні доступ до глобальної мережі є у майже усюди, що дозволяє знизити витрати на підключення. Перевагою також є те, для дзвінків в локальній мережі можливо використовувати внутрішній сервер.

Завдяки певним факторам в IP-телефонії можливо поліпшити якість зв'язку[14]:

- телефонні сервери постійно удосконалюються і алгоритми їх роботи стають більш стійкими до затримок або інших проблем IP-мереж.

- у приватних мережах їх власники мають повним контролем над ситуацією і можуть змінювати такі параметри, як ширина смуги пропускання, кількість абонентів на одній лінії, і, як наслідок, величину затримки.
- мережі з комутацією пакетів розвиваються, і щорічно вводяться нові протоколи і технології, що дозволяють поліпшити якість зв'язку (наприклад, протокол резервування смуги пропускання RSVP).

Розлянемо забезпечення IP-телефонії в розрізі моделі OSI[12].

1) На фізичному рівні здійснюється передача потоку бітів по фізичному середовищю через відповідний інтерфейс. В загалом IP-телефонія на вже існуючу інфраструктуру мережі. Як середовище передачі інформації часто використовують кручену пара категорії 5 (UTP5), одномодовое або многомодовое оптичне волокно, або коаксіальний кабель. Тим самим і реалізується принцип конвергентних мереж.

Для IP-телефонії досить зручною є технологія PoE (Power Over Ethernet) - стандарти IEEE 802.3 af-2003 і IEEE 802.3at-2009, суть якої полягає в забезпеченні живлення пристроїв за допомогою стандартної крученої пари. Більшість сучасних IP-телефонів, наприклад, ряд Cisco Unified IP Phones 7900 Series (рис. 1.12), використовують технологію PoE.

Рисунок 1.12 Cisco Unified IP Phones 7900 Series

При подачі живлення використовують дві кручені пари 100BASE-TX, проте деякі виробники можуть використовувати чотири, досягаючи потужності до 51 Ватт. Також здійснюється постійний контроль перевантажень.

2) Згідно зі специфікацією IEEE 802 канальний рівень поділяється на два підрівні:

- MAC (Media Access Control) - забезпечує взаємодію з фізичним рівнем;
- LLC (Logical Link Control) - обслуговує мережевий рівень.

На канальному рівні працюють комутатори - пристрої, що забезпечують з'єднання декількох вузлів комп'ютерної мережі та розподіл фреймів між хостами на основі фізичної (MAC) адресації.

Необхідно згадати механізм віртуальних локальних мереж (Virtual LoCal Area Network). Дана технологія дозволяє створювати логічну топологію мережі незважаючи на її фізичні властивості. Досягається це тегуванням трафіку, що докладно описано в стандарті IEEE 802.1Q.

В контексті IP-телефонії відзначимо Voice VLAN, широко що застосовується для ізоляції голосового трафіку, що генерується IP-телефонами, від інших даних.

Її використання доцільно з двох причин:

- Безпека. Створення окремої голосової VLAN зменшує ймовірність перехоплення і аналізу голосових пакетів.
- Підвищення якості передачі. Механізм VLAN дозволяє задати високий пріоритет голосовим пакетам, і, як наслідок, поліпшити якість зв'язку.

3) На мережевому рівні визначається, яким шляхом дані досягнутий одержувача з тією чи іншою IP-адресою. Основний маршрутизації протокол - IP (Internet Protocol), на основі якого і побудована IP-телефонія, а також всесвітня мережа Інтернет. Також існує безліч динамічних протоколів маршрутизації, наприклад OSPF (Open Shortest Path First) - внутрішній протокол, заснований на поточний стан каналів зв'язку;

Спеціальні VoIP-шлюзи (Voice Over IP Gateway) забезпечують підключення звичайних аналогових телефонів до IP-мережі. Вони мають вбудований

маршрутизатор, що дозволяє вести облік трафіку, авторизувати користувачів, автоматично видавати IP-адреси, управляти смугою пропускання.

Стандартних функції VoIP-шлюзів:

- Функції безпеки (створення списків доступу ACL, авторизація);
- Підтримка факсимільного зв'язку;
- Підтримка голосової пошти;
- Підтримка протоколів H.323, SIP (Session Initiation Protocol).

Для боротьби з можливими затримками передачі по IP необхідно використовувати додаткові засоби, наприклад протоколи організації черг - для пріорітетних голосових даних.

Як правило, для досігнення даних цілей на маршрутизаторах використовуються проторол організації черг з малою затримкою (LLQ - Low-Latency Queuing), або зважена організація черг на основі класів (CBWFQ - Class-Based Weighted Fair Queuing). А також, використовуються схеми маркування із заданням пріоритетів для голосових даних, як найбільш важливих для передачі[4, 14].

4) Для транспортного рівня характерні:

- Сегментація даних додатків верхнього рівня моделі OSI;
- Забезпечення наскрізного з'єднання;
- Гарантія надійності даних.

Основні протоколи транспортного рівня - TCP, UDP, RTP. Основна відмінність UDP і RTP від TCP полягає в тому, що вони не забезпечують надійність доставки даних, але затримки будуть меншими. Телефонний зв'язок надзвичайно залежний від затримок передачі, але менш чутливий до втрат пакетів[13].

У мережах, що не забезпечують гарантовану якість обслуговування, пакети можуть втрачатися, може змінюватися порядок їх надходження, дані, що передаються в пакетах, можуть спотворюватися. Для забезпечення надійної

доставки інформації, що передається в цих умовах використовуються різні процедури транспортного рівня.

При передачі цифрових даних для цієї мети застосовується протокол TCP (Transmission Control Protocol). Даний протокол забезпечує надійну доставку даних і відновлює вихідний порядок проходження пакетів. Якщо в пакеті виявлено помилку, або пакет втрачається, процедури TCP надсилають запит на повторну передачу.

Для додатків аудіо- та відеоконференцзв'язку затримки пакетів набагато більшою мірою впливають на якість сигналу, ніж окремі спотворення даних. Відмінності в затримках можуть призводити до появи пауз. Тоді для додатків необхідний інший протокол транспортного рівня, що забезпечує відновлення початкової послідовності пакетів, їх доставку з мінімальною затримкою, відтворення в реальному часі в точно задані моменти, розпізнавання типу трафіку, груповий або двосторонній зв'язок.

Таким протоколом є транспортний протокол реального часу RTP (Real-Time TransPort Protocol). Даний протокол регламентує передачу мультимедійних даних в пакетах через ITT на транспортному рівні і доповнюється протоколом управління передачею даних в реальному масштабі часу RTCP (Real-Time Control Protocol).

Протокол RTCP, в свою чергу, забезпечує контроль доставки мультимедійних даних, контроль якості обслуговування, передачу інформації про учасників поточного сеансу зв'язку, управління та ідентифікацію, і іноді вважається частиною протоколу RTP[13].

5-7) Процеси на даних рівнях сеансовому, представлення та додатків тісно пов'язані між собою, і описувати їх без поділу на підрівні буде логічніше.

H.323 - включає безліч інших стандартів, які відповідають за певні аспекти передачі інформації. Деякі з них - стандарти аудіо- та відеокодеків, мають широке застосування не тільки в IP-телефонії. Стосовно протоколів RTP/RTCP - вони складають основу стандарту H.323 та орієнтовані на забезпечення саме IP-технології, лежать в основі організації IP-телефонії. Рекомендації H.323 досить докладно описують способи організації мультимедійних конференцій, охоплюючи

сервіси передачі голосу, відео і комп'ютерних даних в пакетних мережах з негарантованої доставкою.

До основних компонентів набору відносяться описані нижче протоколи[15].

H.225 - описує процес встановлення, підтримки і завершення з'єднання. Обмін повідомленнями відбувається по протоколу TCP.

RAS (Registration, Admission, Status) - відповідає за реєстрацію пристроїв в мережі, контроль доступу до ресурсів, контроль смуги пропускання, необхідної для сеансу зв'язку, і контроль стану пристроїв в мережі. Працює по протоколу UDP.

H.245 - відповідає за обмін інформацією, необхідною для узгодження параметрів логічних каналів для передачі медіа-потоків, власне голосу або відео. Сюди входить, наприклад, узгодження кодеків, номерів UDP-портів і так далі. Обмін відбувається по протоколу TCP.

H.450.x - відповідає за забезпечення додаткових функцій, як Hold, Transfer і т.д..

Архітектура H.323 складається з чотирьох функціональних компонентів: термінал, шлюз, гейткіпер, пристрій багатокористувацьких конференцій.

Протокол SIP (Session Initiation Protocol), описаний в рекомендаціях RFC 2543, регламентує встановлення і завершення мультимедійних сесій - сеансів зв'язку, в ході яких користувачі можуть говорити один з одним, обмінюватися відеоматеріалами та текстом, спільно працювати над додатками і т. д. SIP та супутні йому протоколи народилися і розвиваються в рамках IETF - головного органу стандартизації Інтернету.

Ннабір рекомендацій RFC, які відносяться до SIP-архітектури, налічує декілька десятків документів. SIP клієнт-серверний протокол, робота якого складається з низки запитів і відповідей, причому всі SIP-заголовки передаються в форматі ASCII-тексту, а тому легко зчитаються. SIP дозволяє використовувати логічну адресацію (URL) на базі протоколу TCP або UDP.

1.6 Висновки з розділу 1

Досліджено концепцію побудови IP-мережі. Різні види інформації мультимедійної мережі вимагають підтримки відповідних механізмів забезпечення якості обслуговування QoS. Якість обслуговування загалом описує вимоги додатку до роботи мережвої служби.

Проаналізовані вимоги QoS по відношенню до таких різних типів трафіку, таких як голос, відео, дані. Якщо ці вимоги будуть дотримані, то додаток буде ефектифно працювати. Тому впровадження механізмів забезпечення якості обслуговування QoS - одне із пріорітетних завдань при розгортанні мережі. Однак, для того щоб вибрати який підхід необхідно впровадити, в другому розділі будуть проаналізовні технології та інструменти для управління мережевим трафіком.

РОЗДІЛ 2. АНАЛІЗ ЗАСОБІВ УПРАВЛІННЯ МЕРЕЖНИМ ТРАФІКОМ

2.1 Потокова передача даних

Потокова передача медіаданих - це передача відео або аудіо даних, які надсилається у стислій формі через мережу і відтворюється в режимі реального часу, а не зберігається на носіях типу жорсткого диску.

Пре передачі потокового даних для користувача відсутня необхідність очікування повного завантаження файлу для його відтворення. Користувачі можуть призупинити, перемотати назад або вперед, так само, як і з завантаженим файлом, за винятком тих випадків, коли вміст транслюється в прямому ефірі.

Перевагами потокової передачі є:

- користувачі можуть користуватись інтерактивними програмами, такими як пошук відео та персоналізовані списки відтворення;
- дає можливість постачальнику контенту моніторити, які користувачі завантажуюсть і скільки;
- забезпечує ефективне використання пропускної здатності, оскільки лише частина переданого файлу - це частина, яку переглядають;
- забезпечує кращий контроль над інтелектуальною власністю, оскільки відеофайл не зберігається при відтворенні.

У прямому ефірі відеосигнал перетворюється на стислий цифровий сигнал і передаються з веб-сервера у вигляді багатоадресної передачі(multiCast), одночасно надсилаючи один файл декільком користувачам.

Потокові дані передаються за допомогою серверної програми, які отримуються та відображаються в режимі реального часу за допомогою клієнтської програми, яка називається мультимедійним програвачем. Медіа-плеєр може бути частиною браузера, плагіна, окремої програми. Часто, відеофайли поставляються з вбудованими мультимедійними програвачами. Наприклад, у вбудованих програвачах Flash відттворюється Youtube-відео.

2.2 Класифікація мережного трафіку

У телекомунікаційних мережах трафік зазвичай є неоднорідним і складається з багатьох потоків програм і утиліт. Багато таких додатків є унікальними та мають власні вимоги стосовно показників якості обслуговування, таких як затримка, джитер, втрата пакетів та ін. Якщо вимоги не будуть виконані, то якість та зручність використання цих програм суттєво впаде. Виконання цих вимог у мережі, що має величезну смугу пропускання, є досить легким завданням, але зазвичай існує обмеження пропускної здатності, тому існує необхідність використовувати наявні ресурси максимально ефективно.

Таким чином, управління трафіком необхідно, для правильного визначення пріоритетів потоків різних додатків у межах пропускної здатності та забезпечити виконання вимог до якості обслуговування. Крім того, правильне визначення приналежності трафіку до певних програм та протоколів є важливим для системних адміністраторів з точки зору реалізації відповідної політики безпеки. Важливим є і сприйняття користувача - хоча програма може дозволити великі затримки або джиттер, користувач може бути дуже чутливим до довгого часу очікування. Тому для управління мережевим трафіком необхідний розумний баланс пріоритетів.

Класифікація трафіку - це лише перший крок, який допомагає ідентифікувати різні програми та протоколи, які існують у мережі. Потім можуть виконуватися різні дії, такі як моніторинг, виявлення, контроль та оптимізація, на визначений трафік з кінцевою метою підвищення ефективності мережі. Як правило, коли пакети класифікуються (ідентифікуються) як такі, що відносяться до певної програми або протоколу, вони позначаються або позначаються. Ці маркування або прапорці допомагають маршрутизатору визначати відповідні службові правила, які застосовуються для цих потоків.

Існує два основних підходи до класифікації трафіку (рис. 2.1.):

- на основі вмісту - пакети класифікуються на основі полів корисного навантаження, таких як порти четвертого рівня моделі OSI;

- на основі статистичного аналізу, який використовує статистичний аналіз поведінки трафіку, як тривалість між прибуттям двох пакетів, тривалість і т.д.

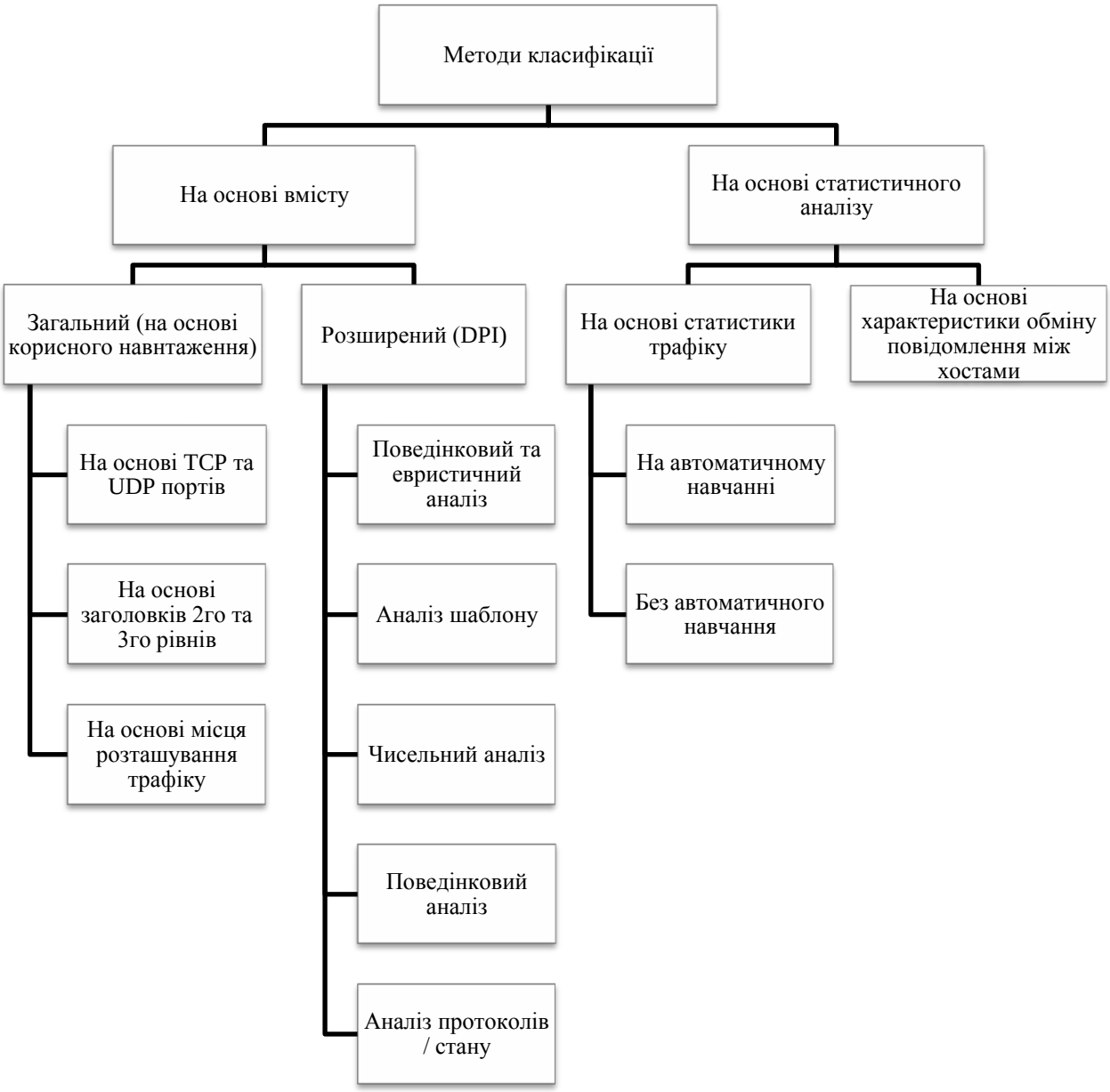


Рисунок 2.1. Методи класифікації мережевого трафіку

2.2.1 Класифікація трафіку на основі вмісту

Метод на основі корисної навантаження є найбільш поширеним. Однак, він не працює з зашифрованим і тунельним трафіком. Даний метод класифікації може бути поділений на загальний аналіз корисного навантаження та розширений аналіз.

Загальний підхід до класифікації трафіку ґрунтується на інформації в заголовку IP. Також існує метод класифікації на основі місця розташування трафіку (на вхідному інтерфейсі), але він широко не використовується.

При класифікації потоків трафіку на рівні 2 і 3 використовуються інтерфейси, списки контролю доступу і карти класів. Маркування означає додавання деякого значення у заголовок пакету. Пристрої, які приймають пакет, порівнюють значення цього поля зі значенням, визначеним політикою приорітизації. Маркування необхідно проводити максимально близько до вихідного пристрою. Рішення про маркування трафіку на рівнях 2 і 3 має прийматися з урахуванням факторів:

- Маркування рівня 2 для кадрів можна виконувати для не тільки для IP-трафіку.
- Маркування рівня 2 для кадрів є єдиним можливим варіантом реалізації якості обслуговування для комутаторів 2го рівня.
- Маркування рівня 3 забезпечує наскрізну передачу даних про якість обслуговування.

У таблиці 2.1 описуються деякі поля маркування, які використовуються в різних технологіях. 802.1Q - це стандарт IEEE, який підтримує мережі VLAN в мережі Ethernet. Формат кадру Ethernet 802.1Q зображений на рисунку 2.2. Цей стандарт також включає схему пріоритезації якості обслуговування IEEE 802.1P.

Табл.2.1 Маркування трафіку для забезпечення якості обслуговування

Технології	Рівень	Поле маркування	Ширина в бітах
Ethernet (802.1Q, 802.1P)	2	Класс обслуговування (CoS)	3
802.11 (Wi-Fi)	2	Ідентифікатор трафіку беспроводової мережі (TID)	3
MPLS	2	Експериментальне (EXP)	3
IPv4 и IPv6	3	Пріоритет IP-трафику	3
IPv4 и IPv6	3	Точка коду дифференційованих сервісів (DSCP)	6

Ідентифікатор протоколу тегів (TPID) на даний момент фіксований і має значення 0x8100. Контрольні дані тегів (TCI) включають 3-бітове поле пріорітет користувача (User Priority), яке визначає маркування відповідно до класу обслуговування (CoS). Маркировка CoS дозволяє маркувати кадр пріоритетом від нуля (найнищий пріоритет) до семи, як показано на в таблиці 2.2.

Маркування на рівні 3 забезпечується за допомогою 8-бітного поля в заголовку пакету, що дозволяє маркувати пакети. Для вказаних цілей у протоколі IPv4 використовується поле Тип послуги (TOS), а у протоколі IPv6 -поле Клас трафіку (TraffiC Class).

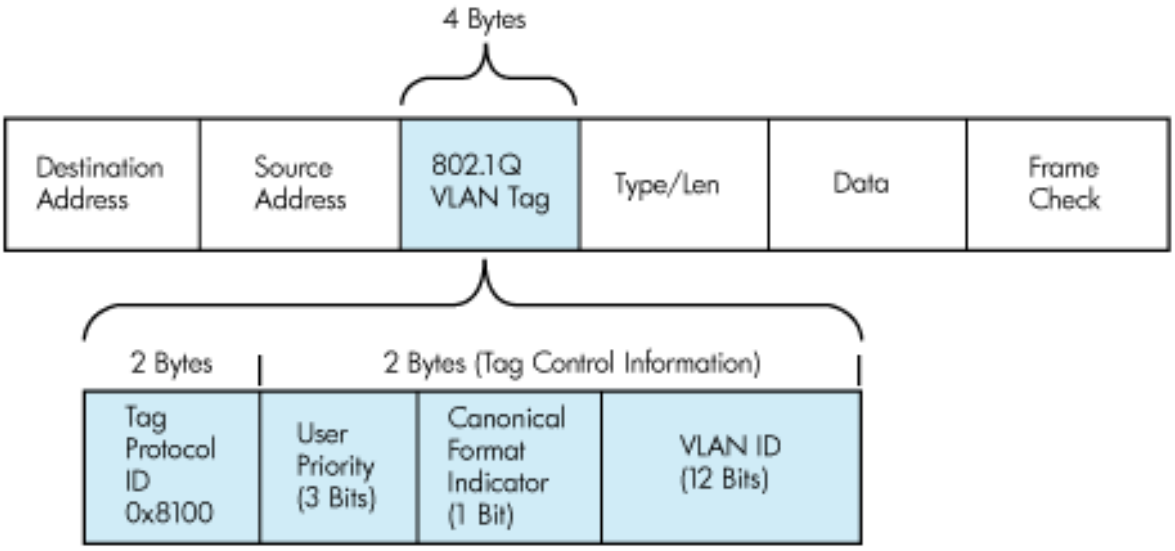


Рисунок 2.2 Формат кадру Ethernet 802.1Q

При використанні моделі DiffServ пакет позначається з використанням 6 біт, який називають битами DSCP. Шість біт визначають максимально можливий номер класів обслуговування, рівний 64. Маршрутизатори з підтримкою DiffServ реалізують поведінку для вузлів PHB (Per-Hop Behavior), яка визначає властивості передачі пакетів, пов'язаних із класом трафіку. Категорії PBH описані в таблиці 2.3.

Таблиця. 2.3 Значення класу обслуговування (CoS)

Значення	Опис
0	Дані з низьки пріорітетом
1	Дані з середнім пріорітетом
2	Дані з високим пріоритетом
3	Сигнальний трафік
4	Відеоконференція
5	Голосовий трафік
6	Зарезервовано
7	Зарезервовано

Усі загальні методи класифікації базуються на основі IP-адреси призначення, IP-адреси відпавника чи IP-протоколу та ін. Однак, вони обмежені у своїх можливостях, оскільки перевірка обмежена тільки заголовком IP.

Аналогічним чином, класифікація на базі портів четвертого рівня. Виділенням і реєстрацією портів займається організація Internet Assigned Numbers Authority (IANA), однак часто зустрічаються випадки їх неофіційного застосування.

Перевагою методу є простота реалізації та висока швидкість роботи, а недоліком, те що не всі поточні програми використовують стандартні порти. Деякі програми навіть можуть працювати через визначені порти інших програм (наприклад, такі програми як швидкі повідомлення (IM) можуть працювати через порт 80, який зазвичай використовується для HTTP).

Таблиця 2.4 Категорії PBH

Категорія PHB	Опис
За замовчуванням	• Використовується для моделі обслуговування без гарантії доставки. • Крайні ліві біти DSCP рівні 000xxx.
Прискорене пересилання (ExPedited Forwarding, EF)	• Використовується для прискореного обслуговування, забезпечуючи малі втрати, низькі затримки, малий джиттер і гарантовану пропускну здатність для передачі відео і голосу. • Крайні ліві біти DSCP рівні 101xxx.
Гарантоване пересилання (Assured Forwarding, AF)	• Використовується для забезпечення гарантованої пропускної здатності. • Має 4 підкласа (AF1, AF2, AF3 и AF4). • Крайні ліві біти DSCP рівні 001xxx, 010xxx,011xxx или 100xxx.
Селектор класу	• Використовується для забезпечення сумісності з пристроями, не підтримують DiffServ. • Біти DSCP з 2-го по 4-й рівні xxx000.

Розширені методи класифікації спираються на глибокий аналіз пакетів (DPI). Існують різноманітні методи DPI, такі як аналіз шаблонів або аналіз поведінки, що є більш надійним, ніж загальні методи класифікації.

1. Аналіз шаблону. Деякі програми додають певні шаблони (байти, символи, рядок) в корисне навантаження пакетів, які можуть використовуватися для ідентифікації таких протоколів. Шаблони можуть бути присутніми в будь-якій позиції в пакеті. Проте не всі протоколи вставляють спеціальні шаблони, рядки чи символи в пакети, і тому цей підхід для них не буде працювати.

2. Чисельний аналіз. Включає в себе вивчення числових характеристик пакетів, таких як розмір корисного навантаження, кількість пакетів відповідей та інше. Версії Skype 2.0 і раніші є хорошими прикладами для такого аналізу. Запит клієнта - це 18-байтне повідомлення, і відповідь, яку він отримує, зазвичай 11 байт. Оскільки аналіз може бути розподілений на кілька пакетів, рішення про класифікацію може зайняти більше часу.

3. Поведінковий та евристичний аналіз. Іноді аналіз поведінки трафіку дасть змогу краще зрозуміти роботу програм. Ця поведінка може бути використана для класифікації. Багато антивірусних програм використовують ці методи для виявлення вірусів та червів.

4. Протокол аналізу стану. У деяких програмах протокол виконує певну послідовність кроків або дій. Наприклад, на запит GET FTP-протоколу від клієнта відправляється відповідь з сервера. Така відповідність протоколу може бути використана для класифікації такого трафіку.

Оскільки більшість програм запускає шифрування трафіку, класифікація стає досить складним процесом. За допомогою шифрування вся інформація верхнього рівня стає невидимою для механізмів DPI. Методи аналізу поведінки та евристичного аналізу можуть допомогти ідентифікувати ідентифікувати зашифрований трафік.

Часто ці методи разом використовується декілька вище вказаних методів для забезпечення найбільш точної ідентифікації мережевого трафіку.

2.2.2 Класифікація на основі статистичного аналізу

Статистичні методи можна поділити на дві групи: на основі характеристики обміну повідомлення між хостами і на основі статистистики трафіку. Основна мета першого методу полягає у визначенні, які додатки створюють створюють основний потік трафіку. Аналізуючи, як в рамках мережі взаємодіють хости, можна визначити які види додатків запущені на хості. Підхід статистичних методів спирається на статистичні характеристики трафіку для ідентифікації додатка. Припущення, що

лежать в основі таких методів, полягають в тому, що мережевий трафік має статистичні характеристиками, які є унікальними для певних класів додатків і дозволяють розділити різні види додатків.

Статистичні алгоритми в залежності від підходу до класифікації можна розділити на дві групи: методи класифікації або навчання з учителем та методи кластеризації або навчання без учителя. Розглянемо детальніше етапи застосування методів машинного навчання з учителем для класифікації мережевого трафіку.

Застосування методів машинного навчання для класифікації *IP*-трафіку.

У разі, коли машинне навчання застосовується для класифікації *IP*-трафіку, ряд понять змінюють свій сенс. З метою подальшого обговорення визначимо наступні три терміни, що відносяться до потоків:

- потік або однонапрямлений потік : ряд пакетів, що розділяють однаковий кортеж з п'яти елементів: *IP*- адреси джерела і одержувача, номера портів джерела і одержувача, номер протоколу;
- двонаправлений потік: пара однонапрямлених потоків, що протікають в протилежних напрямах, між тими ж самими *IP*- адресами відправника і отримувача та портами;
- призначення і портами; повний потік: двонаправлений потік, захоплений за увесь його час існування від створення до завершення з'єднання.

Клас зазвичай вказує на *IP*-трафік, сформований додатком або групою додатків. У якості зазвичай виступають числові атрибути вирахувані на основі мережевих пакетів. Не усі ознаки однаково впливають на процес класифікації, тому на практиці класифікатори вибирають найменшу множину ознак, яке приведе до ефективного розділення.

Рис. 2.3, 2.4 ілюструють кроки, пов'язані з побудовою класифікатора трафіку, що використовує алгоритм навчання з учителем (контрольоване машинне навчання).

Рис. 2.3 охопив повний процес навчання і перевірки, які відбуваються в класифікаційній моделі. Оптимальний підхід до алгоритму навчання з учителем повинен передбачати заздалегідь класифіковані зразки двох типів *IP*- рафіку:

- трафіку, що відповідає класу, який хочемо пізніше ідентифікувати в мережі;

- трафіку від інших застосувань, які, можливо, зустрінуться в майбутньому (що часто називається таким, що втручається трафіком).

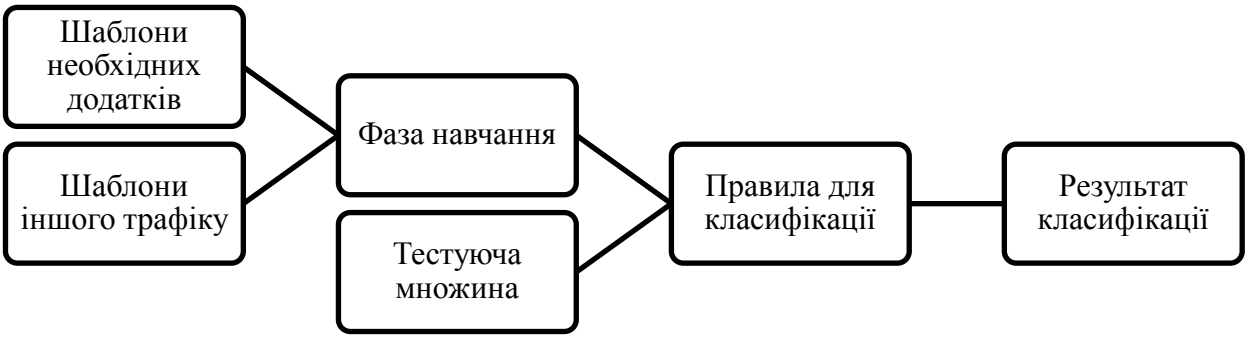


Рисунок 2.3 Навчання та тестування для двукласового класифікатора трафіка з вчителем.

Рисунок 2.3 детально зупиняється на послідовності подій, пов'язаних з навчанням класифікатора з учителем. Спочатку збирається суміш "трас трафіку", яка включає екземпляри застосування, що цікавить нас, і екземпляри інших застосувань (таких як, *HTTP*, *DNS*, *SSH* і/або *P2P*), що втручаються. Крок "обробка статистики потоку" включає обчислення статистичних властивостей цих потоків і підводить до початку формування ознак.

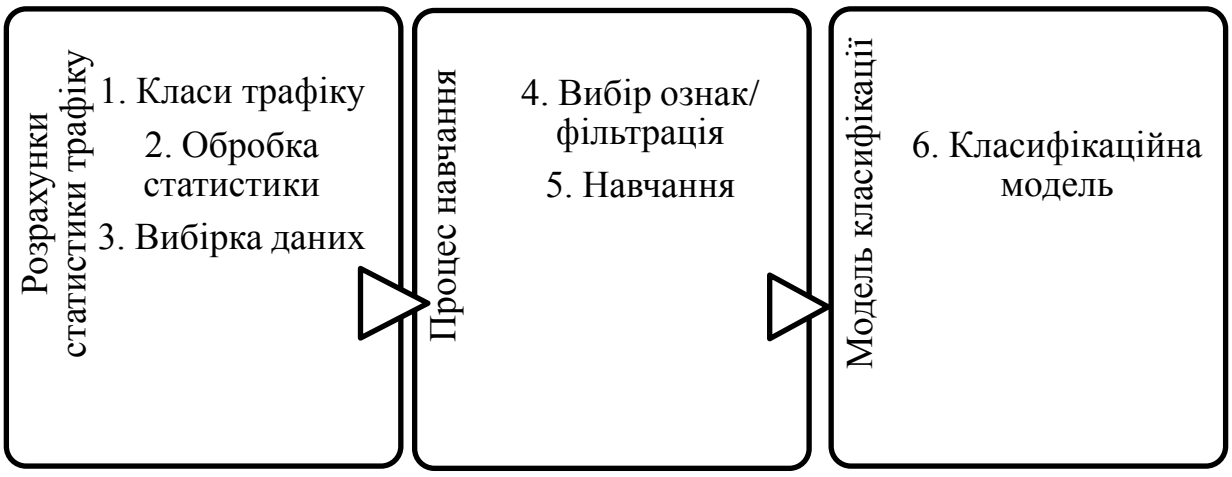


Рисунок 2.4 Навчання класифікатора з вчителем

Наступний необов'язковий крок - "здійснення вибірки даних", розроблений, щоб звузити зону пошуку для повчального алгоритму, коли він стикається з надзвичайно великими повчальними наборами даних (трасами трафіку). Крок здійснення вибірки витягає статистику з підмножини випадків 16 різних прикладних класів, і передає їх класифікаторові, який буде використовуватися в повчальному процесі. Крок фільтрації/вибору ознак бажаний, щоб обмежити число ознак дійсно використовуваних при навчанні класифікатора, і, таким чином, створювати модель класифікації. Вихідний сигнал на рис.2.4 - модель класифікації.

Перехресна перевірка (чи багатошарова перехресна перевірка) може використовуватися, щоб зробити результати оцінки точності під час фази навчання.

Проте якщо початковий набір даних складатиметься з *IP*-пакетів, зібраних в те ж самий час і в тій же самій вимірюваній мережевій точці, то у випадку початковий набір даних повинен би містити суміш трафіку, зібраного в різне час і різних точках мережі, або використати повністю незалежно зібрані повчальні і тестуючі набори даних.

Трафік, зібраний в реальному часі, використовується, щоб вичислити статистику потоку, від якої визначаються ознаки, що передаються потім в модель класифікації. Тут ми припускаємо, що набір ознак, вичислених від захопленого трафіку, обмежений оптимальним набором ознак, визначених в час навчання. На виході класифікатора вказується, які потоки, передбачається, є членами класу (як визначено моделлю), що цікавить. Додаткова реалізація може дозволити моделі оновлюватися в реальному часі. Для контролю над тестуванням і оцінкою точності можуть використовуватися автономні траси трафіку замість захоплення в реальному часі.

Навчання вимагає апріорної класифікації (чи маркіровки) потоків усередині повчальних наборів даних. Тому схему навчання з учителем можна використати для визначення ознак (чи груп) застосувань, що цікавляться. Проте, як було відмічено раніше, класифікатор краще всього працює у разі навчання його на зразках усіх класів, очікуваних зустрітися на практиці. Отже, його виконання може бути погіршено або спотворено, якщо не провести навчання на зразку трафіку, що змішав

чи в мережі з'явиться трафік раніше невідомих застосувань. Тому при оцінці схем навчання з учителем варто враховувати, яким чином класифікатор і як користувач виявить новий тип додатків.

2.3 Класифікація засобів управління мережевим трафіком

2.3.1 Динамічна та статична маршрутизація

Маршрутизація - процес визначення маршруту прямування інформації між мережами. Маршрутизатор приймає рішення, що базується на *IP*-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують *IP*-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж[18].

Загалом маршрутизація ділиться на два типи:

- статична маршрутизація - маршрути задаються вручну адміністратором;
- динамічна маршрутизація - маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації — *RIP*, *OSPF*, *EIGRP*, *IS-IS*, *BGP*, *HSRP* та ін., які отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі.

Оскільки статичні маршрути конфігуруються вручну, будь-які зміни мережної топології вимагають участі адміністратора для додавання і видалення статичних маршрутів відповідно до змін. У великих мережах підтримка таблиць маршрутизації вручну може вимагати величезних витрат часу адміністратора. У невеликих мережах це робити легше. Статична маршрутизація не має можливості масштабування, яку має динамічна маршрутизація через додаткові вимоги до налаштування і втручання адміністратора. Але і у великих мережах часто конфігуруються статичні маршрути для спеціальних цілей у комбінації з протоколами динамічної маршрутизації, оскільки статична маршрутизація є стабільнішою і вимагає мінімум апаратних ресурсів маршрутизатора для обслуговування таблиці[4,18].

Динамічні маршрути виставляються іншим чином. Після того, як адміністратор активізував і налаштував динамічну маршрутизацію за одним з протоколів, інформація про маршрути оновлюється автоматично в процесі маршрутизації після кожного отримання з мережі нової інформації[4,18].

RIP - так званий дистанційно-векторний протокол, який оперує переходами (хопами) як метрикою маршрутизації. Максимальна кількість хопів, дозволений *RIP* - 15 (метрика 16 означає «нескінченно велику метрику», тобто недосяжний сегмент мережі). Кожен *RIP*-маршрутизатор за замовчуванням сповіщає в мережу свою повну таблицю маршрутизації раз на 30 секунд, генеруючи досить багато трафіку на низькошвидкісних лініях зв'язку.

У *RIP* - не найкраще рішення для вибору в якості протоколу маршрутизації, тому що його можливості поступаються сучаснішим протоколам, таким як *EIGRP*, *OSPF*. Обмеження в 15 хопів не дає застосовувати його у великих мережах. Перевага цього протоколу — простота конфігурування. Внаслідок простоти його підтримують практично всі маршрутизатори початкового рівня.

OSPF(англ. *Open Shortest Path First*) — протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (*link-state technology*), що використовує для знаходження найкоротшого шляху Алгоритм Дейкстри (*Dijkstra's algorithm*).

Протокол *OSPF* був розроблений *IETF* в 1988 році. Остання версія протоколу представлена в *RFC* 2328. Протокол *OSPF* являє собою протокол внутрішнього шлюзу (*Interior Gateway Protocol - IGP*). Протокол *OSPF* поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи.

Властивості *OSPF*:

- висока швидкість збіжності;
- підтримка мережних масок змінної довжини *VLSM;*
- відсутність обмежень досяжності;
- оптимальне використання пропускної здатності мережі;
- оптимальний вибір шляху маршрутизації.

Згідно з *RFC* 2328 [17] є незапатентований тобто відкритий для громадськості протокол, таким же, як є протокол *RIP*. Але *OSPF* на відміну від *RIP*, має значно більшу швидкість збіжності (рекалькуляції таблиці маршрутизації), немає обмеження на довжину шляху 15-ма хопами, враховує пропускну здатність мережі при виборі маршруту. Все це робить *OSPF* потужним, масштабованим протоколом маршрутизації.

Enhanced Interior Gateway Routing Protocol (*EIGRP*) - це пропрієтарний протокол маршрутизації, що базується на старому протоколі *IGRP*. *EIGRP* - дистанційно-векторний протокол маршрутизації, що був оптимізований для зменшення нестабільності протоколу після змін топології мережі, уникнення проблеми зациклення маршруту та більш ефективного і економного використання потужностей маршрутизатора. Роутери, що підтримують протокол *EIGRP* також підтримують і *IGRP* та перетворюють маршрутну інформацію для *IGRP*-сусідів з 32-бітної метрики *EIGRP* у 24-бітну метрику стандарту *IGRP*. Алгоритм визначення маршруту базується на алгоритмі Дейкстри пошуку в глибину на графі. *EIGRP* обчислює і враховує 5 параметрів для кожної ділянки маршруту між вузлами мережі[4]:

- *Total Delay* - Загальна затримка передачі (з точністю до мікросекунди);
- *Minimum Bandwidth* - Мінімальна пропускна спроможність (в Кб/с - кілобіт/секунду);
- *Reliability* - Надійнсть (оцінка від 1 до 255; 255 найбільш надійно);
- *Load* - Завантаження (оцінка від 1 до 255; 255 найбільш завантажено);
- *Maximum Transmission Unit* (*MTU*) (не враховується при обчисленні оптимального маршруту, береться до уваги окремо) - максимальний розмір блоку, що можливо передати по ділянці маршруту.

EIGRP також обчислює кількість вузлів для кожного маршруту, проте не використовує це в обчисленні маршруту. Це лише перевіряється з вбудованим максимумом на маршрутизаторі *EIGRP* (за замовчанням це встановлюється на 100 і може бути змінено на будь-яке значення між 1 і 255). Якщо число хопів для певного вузла вище, ніж максимум, вузол вважатиметься як недосяжний маршрутизатором.

BGP (англ. *Border Gateway Protocol*, укр. Протокол Граничного Шлюзу) з 1994 року єдиний протокол маршрутизації між автономними системами в глобальній мережі Інтернет, а його розширена версія *MBGP* (*Multiprotocol BGP*) використовується в *MPLS*-мережах *IT*-провайдерів.

BGP є протоколом міждоменної маршрутизації та належить до класу дистанційно-векторних протоколів. Як протокол міждоменної маршрутизації використовується усіма інтернет-провайдерами, а також великими компаніями та організаціями, які мають власні публічні номери автономних систем (*ASN*) та користуються послугами більш ніж одного інтернет-провайдера (мултіхомінг) або мають прямі *IP*-з'єднання з багатьма іншими великими компаніям, що також мають власні публічні номери автономних систем, без використання послуг інтернет-провайдерів.

На відміну від класичного дистанційно-векторного протоколу *RIP*, метрикою якого є кількість хопів (відрізків шляху) між маршрутизаторами, найкращий маршрут *BGP* обирається по точно визначеному пріоритету атрибутів, одним із яких, але не найпріоритетнішим, є кількість хопів між автономними системами - найкоротший шлях між автономними системами (англ. *shortest AS Path*). Тому іноді цей протокол зараховують до окремого класу шляхо-векторних протоколів.

HSRP (англ. *Hot Standby Router Protocol*) - фірмовий протокол *Cisco*, призначений для збільшення доступності маршрутизаторів, що виконують роль шлюзу. Це досягається шляхом об'єднання маршрутизаторів в standby групу та призначення їм загальної *IP*-адреси, яка і буде використовуватися як шлюз за замовчуванням для комп'ютерів в мережі.

2.3.2 Управління чергами

Розподіл пропускної здатності трактів передачі мережі може здійснюватися шляхом нормування швидкості *TCP* (*TCP rate shaping*), яке полягає у перехопленні та маніпулюванні розмірами *TCP*-вікна, або за допомогою механізмів управління чергами, а точніше - організації та обслуговування черг на мережних вузлах.

Механізм обслуговування черг шляхом регулювання порядку обслуговування пакетів певного потоку (класу) трафіка дозволяє варіювати частоту їхньої обробки й у такий спосіб виділяти певну пропускну здатність даному потоку (класу). Черги та засоби їхньої обробки є інструментами також управління перевантаженнями, коли мережний пристрій не може передати пакети на вихідний інтерфейс в тому темпі, у якому вони надходять.

Механізми обслуговування черг можуть бути класифіковані за такими ознаками(рис. 2.5)[14,21]:

- реалізований принцип розподілу ресурсів (без розподілу ресурсів, пріоритетний розподіл ресурсів шляхом застосування однойменного обслуговування, пропорційний розподіл у круговому обслуговуванні черг і рівномірний розподіл шляхом реалізації максимінної схеми);
- надання гарантій за обраними параметрами мережного з'єднання (у термінах виділеної пропускної здатності або гарантованої середньої затримки)
- принцип розподілу трафіка по чергах (формування черг на основі потоку або на основі класу);
- режим виконання (розподілений - на процесорах *VIP*-плат або нерозподілений - на центральному процесорі маршрутизатора).

Найчастіше в маршрутизаторах і комутаторах застосовуються такі механізми обслуговування черг[4,19]:

- алгоритм «першим прийшов — першим обслужений» (*First-In-First-Out, FIFO*);
- пріоритетне обслуговування (*Priority Queuing, PQ*);
- справедливе обслуговування (*Fair Queuing, FQ*);
- довільне обслуговування (*Custom Queuing, CQ*);
- обслуговування на основі класу (*Class Based Queuing, CBQ*);
- зважене справедливе обслуговування (*Weighted Fair Queuing, WFQ*);
- зважене справедливе обслуговування на основі класу (*Class Based WFQ, CBWFQ*);
- обслуговування з малою затримкою (*Low LatenCy Queuing, LLQ*);

- зважене кругове обслуговування (*Weighted Round-Robin*, *WRR*) і його модифікації;
- кругове обслуговування з дефіцитом (*Deficit Round-Robin*, *DRR*) і його модифікації.

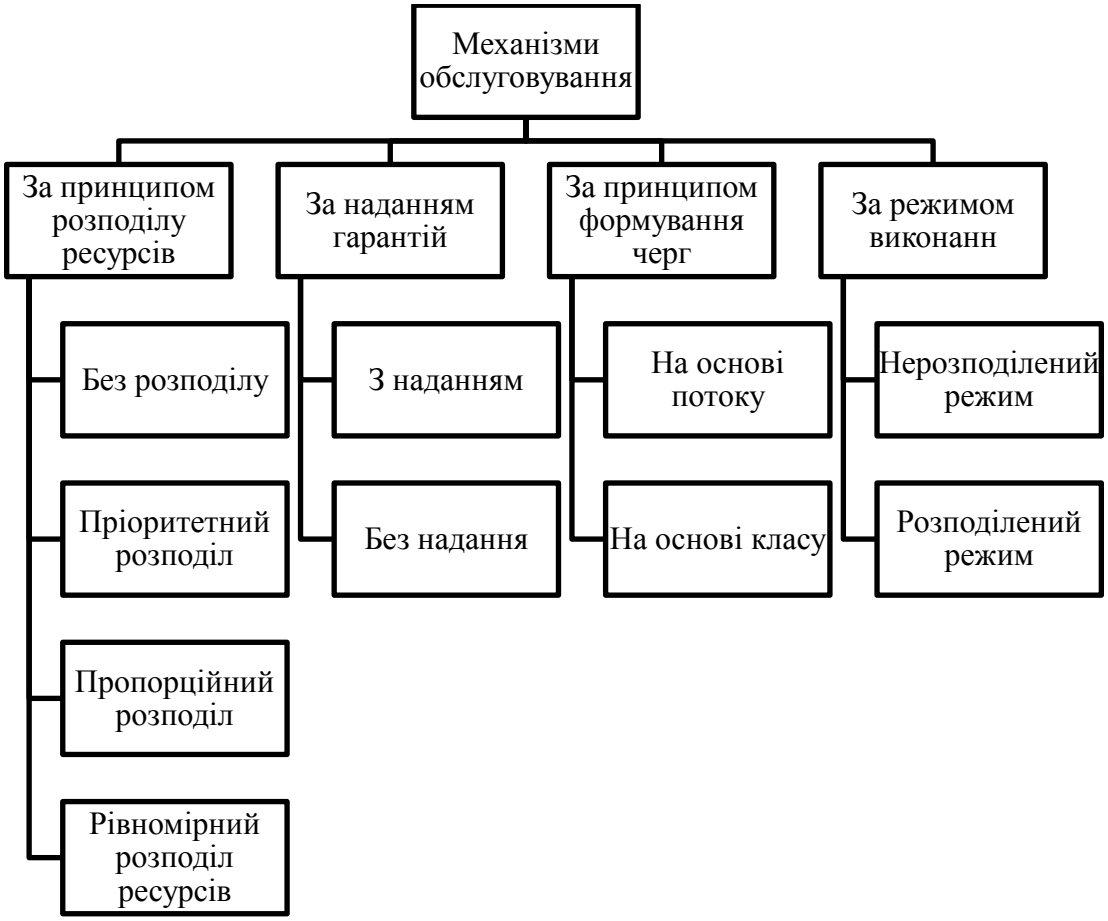


Рисунок 2.5 Класифікація механізмів обслуговування черг.

Для забезпечення *QoS* механізм обслуговування черги повинен мати можливість диференціювання різних потоків пакетів із визначенням рівня їхніх вимог щодо якості обробки. Прикладами механізмів, здатних забезпечити необхідну пропускну здатність у мережах *IP*, є зважений механізм рівномірного обслуговування черг - *WFQ*, зважений механізм рівномірного обслуговування черг на основі класу - *CBWFQ* і на основі потоку - *Flow-Based Distributed Weighted Fair Queuing*. Стисла характеристика основних механізмів обслуговування черг представлена нижче[19,20].

FIFO. У разі використання механізму *FIFO* організується лише одна черга з послідовним проходженням пакетів, що працює за принципом «першим прийшов - першим обслужений».

Пріоритетне обслуговування - *PQ*. Механізм *PQ* забезпечує безумовний пріоритет одних пакетів над іншими. У цьому разі виділяється всього 4 черги: *high, medium, normal* і *low*. Обробка ведеться послідовно (від *high* до *low*), починаючи з високопріоритетної черги і до її повного очищення, не переходить до менш пріоритетних черг. Таким чином, можлива монополізація каналу пакетами з високопріоритетних черг. Трафік, пріоритет якого явно не зазначений, потрапляє у чергу за замовчуванням (*default*).

Довільні черги - *CQ*. Механізм *CQ* забезпечує настроювання черг, тобто передбачається управління часткою пропускної здатності тракту передачі для кожної черги. В цьому механізмі підтримується 16 черг. Системна нульова черга зарезервована для високопріоритетних пакетів (управління, маршрутизація, сигналізація тощо) і користувачеві недоступна. Черги обслуговуються послідовно, починаючи з першої. Кожна черга містить лічильник байтів, що на початку обходу містить задане значення та зменшується на розмір пакета, пропущеного з цієї черги. Якщо лічильник не дорівнює 0, то пропускається наступний пакет цілком, а не його фрагмент, що дорівнює залишку лічильника.

Зважені справедливі черги - *WFQ*. Механізм *WFQ* автоматично розбиває трафік на потоки (*flows*). За замовчуванням кількість дорівнює 256, але може бути й адміністративно змінено. Якщо потоків більше, ніж черг, то в одну чергу вміщує кілька потоків. Приналежність пакета до потоку (класифікація) визначається на основі байта типу обслуговування (*Type of Service, TOS*) із заголовку пакета *IPv4, IP*-адреси джерела, *IP*-адреси призначення, порту джерела та порту призначення (протокол *IP*). Кожний потік використовує окрему чергу.

Цей механізм забезпечує рівномірний (*fair* - справедливий) поділ пропускної здатності каналу між існуючими потоками. Для цього доступна пропускна здатність ділиться на число потоків, і кожний одержує рівну частину. Крім того, кожний потік

одержує свою вагу (*weight*), з певним коефіцієнтом, який обернено пропорційний *IP*-пріоритету (*TOS*).

У підсумку *WFQ* автоматично справедливо розподіляє доступну пропускну здатність, додатково з огляду на *ToS*. Потоки з однаковими *IP*-пріоритетами одержать рівні частки пропускної здатності вихідного каналу; потоки з більшим *IP*-пріоритетом - більшу пропускну здатність. У разі перевантажень ненавантажені високопріоритетні потоки функціонують без змін, а низькопріоритетні перевантажені - обмежуються. За замовчуванням *WFQ* включається на низькошвидкісних інтерфейсах.

Обслуговування черг на основі класів - *CBWFQ*. У рамках механізму *CBWFQ* весь трафік розбивається на 64 класи на підставі таких параметрів: вхідний інтерфейс, список доступу (*Access list*), протокол, значення *DSCP*, мітка *MPLS QoS*. Загальна пропускна здатність вихідного інтерфейсу розподіляється за класами. Виділену кожному класу пропускну здатність можна визначати як в абсолютному значенні (*bandwidth* в *kbit/s*), так і у відсотках (*bandwidth PerCent*) щодо встановленого значення на інтерфейсі. Пакети, які не потрапляють у сконфігуровані класи, потрапляють у клас за замовчуванням, який можна додатково налаштувати і який одержує вільну пропускну здатність, що залишилася. При переповненні черги будь-якого класу пакети даного класу ігноруються.

Черги з низькою затримкою - *LLQ*. Механізм *LLQ* можна розглядати як механізм *CBWFQ* із пріоритетною чергою *PQ* (*LLQ = PQ + CBWFQ*). *PQ* у *LLQ* дозволяє забезпечити обслуговування чутливого до затримки трафіка. *LLQ* рекомендується у разі наявності розмовного (*VoIP*) трафіка. Крім того, цей механізм добре працює під час проведення відеоконференцій.

Необхідною умовою забезпечення мережею гарантованого рівня обслуговування є відсутність у ній перевантажень, тобто стану, при якому мережа нездатна забезпечити погоджені параметри існуючих з’єднань. Механізми запобігання перевантаженню та різних політик відкидання пакетів покликані на основі аналізу мережного трафіка відслідковувати вузькі місця в мережі й не

допускати виникнення на цих ділянках перевантажень. В умовах перевантаження ці механізми забезпечують тільки пільгову обробку пакетів пріоритетного трафіка.

Механізм відкидання пакетів визначає спосіб регулювання довжини черги у разі виникнення її перевантаження або при наближенні до цього стану. Перший випадок відповідає механізму обслуговування черг *FIFO*, який передбачає відкидання всіх вхідних пакетів при досягненні чергою свого максимального значення - це так звана політика «відкидання хвоста» (*tail droP*). У другому випадку задіюються активні механізми управління чергами, які дозволяють запобігти перевантаженню шляхом превентивного відкидання пакетів і тим самим попередити джерело про можливе перевантаження[19,20].

Прикладами активних механізмів управління чергами є алгоритм довільного раннього виявлення (*Random Early Detection, RED*), зважений алгоритм довільного раннього виявлення (*Weighted RED, WRED*). Запобігання перевантаженню в мережах *IP* можливо також за допомогою механізму явного повідомлення про перевантаження (*Explicit Congestion NotifiCation, ECN*), а також шляхом управління розмірами *TCP*-вікна.

На практиці найбільшого поширення набули алгоритми *RED* і *WRED*. Механізм *RED* використовує превентивний підхід щодо запобігання перевантаження мережі та замість очікування фактичного переповнення черги, як при «відкиданні хвоста», *RED* починає відкидати пакети з ненульовою ймовірністю, коли середній розмір черги перевищить певне мінімальне граничне значення. Відкидання пакетів є сигналом *TCP*-джерелу про необхідність зменшити інтенсивність переданого трафіка для відповідного потоку, що досягається за рахунок перезапуску алгоритму повільного старту.

У рамках механізму *RED* уводяться параметри Θmin — мінімальне граничне значення розміру черги, при перевищенні якого в черзі починається процес відкидання пакетів; Θmax - максимальне граничне значення, при перевищенні якого відкидаються всі пакети, які надходять на обслуговування. На рис. 2.5. наведено характерний для механізму *RED* графік залежності ймовірності відкидання пакетів від середнього розміру черги.

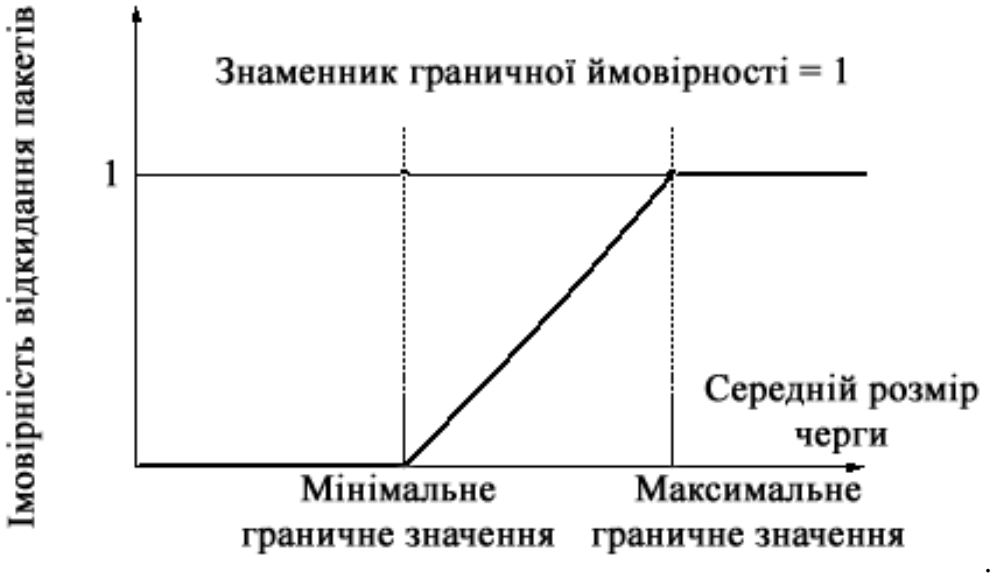


Рисунок 2.5 Залежність імовірності відкидання пакетів від середнього розміру черги для механізму *RED*

Основне призначення механізму *RED* полягає в згладжуванні тимчасових сплесків трафіка та попередженні тривалого перевантаження мережі шляхом неявного повідомлення джерел трафіка про необхідність зниження інтенсивності передачі інформації. Якщо джерела виявлять здатність до взаємодії та одночасно зменшать інтенсивність пакетів переданого трафіка, це допоможе запобігти перевантаженню мережі. В іншому випадку середній розмір черги досить швидко досягне максимального граничного значення, що приведе до відкидання всіх пакетів.

Зважений алгоритм довільного раннього виявлення *WRED* є модифікацією алгоритму *RED* і надає різні рівні обслуговування пакетів залежно від імовірності їхнього відкидання та забезпечує виборчу установку параметрів механізму *RED* на підставі значення поля *IP*-пріоритету. Інакше кажучи, алгоритм *WRED* передбачає можливість більш інтенсивного відкидання пакетів, які належать до певних типів трафіка, і менш інтенсивного відкидання всіх інших пакетів.

2.3.3 Профілювання мережевого трафіку

Обмежувач (*Policer*) відповідно обмежує потік трафіку до потрібної величини методом простого відкидання пакетів, що поступають зі швидкістю, що виходить за рамки. Може працювати на інтерфейсах, як на вхідних, так і на вихідних. Коротко можна охарактеризувати як обмежувач інтенсивності методом відкидання при перевищенні заданої швидкості[4].

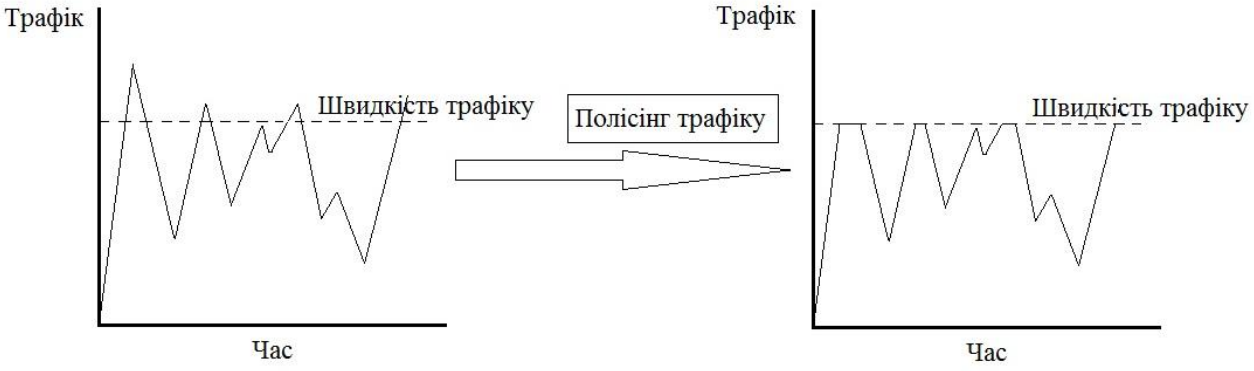


Рисунок 2.6. Трафік полісінг

Призначення застосування : обмеження трафіку до швидкості контракту, тобто управління інтенсивністю. Слід зазначити, що обмеження трафіку може допомогти і у разі відвертання *DOS* атак.

Сфера застосування : як на вхідних, так і на вихідних портах. Найчастіше на вхідних, оскільки в цьому випадку відкидані пакети не доходять до процесу маршрутизації і таким чином економляться ресурси. До обмежувачів трафіку відноситься механізм *Committed Access Rate* (*CAR*).

Формувач (*Shaper*) зазвичай затримує витікаючий трафік, використовуючи буфер або механізм черг, формуючи потік з потрібними параметрами, виконує функції згладжування. Застосовується для обмеження пропускної спроможності на виході з інтерфейсу. Коротко можна охарактеризувати як обмежувач інтенсивності методом затримки (буферизації пакетів) і подальшої пересилки з погодженою інтенсивністю при перевищенні заданої швидкості.[4]

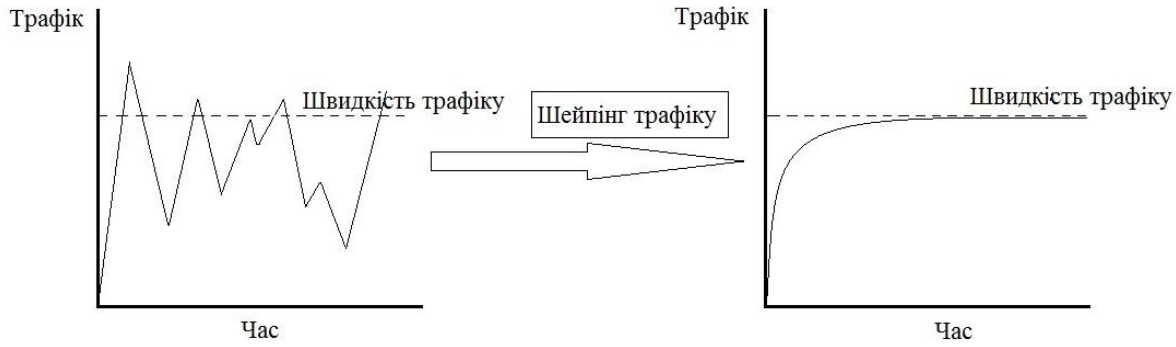


Рисунок 2.7. Трафік шейпінг

Призначення застосування :

- у разі, якщо десь далі в мережі застосовується полісинг, який призводить до відкидання пакетів. Краще заздалегідь "м'яко" обмежити трафік перед полісингом;
- у разі, якщо десь далі в мережі можливе переповнювання вхідних черг, а *QoS* там не налагоджений або неможливий;
- обмеження швидкості доступу до контрактних значень.
- завжди на вихідному інтерфейсі.

2.4 Математична модель TCP-сеансів з урахуванням AQM-алгоритмів

З метою математичного опису одночасно функціонуючих TCP-сеансів з урахуванням класів обслуговування динаміку багатопотокового інформаційного обміну з урахуванням AQM-алгоритмів (Active Queue Management) відображають у вигляді системи рівнянь[23]:

$$\frac{d\lambda_i^k(t)}{dt} = \begin{cases} \text{режим slow start} \\ \left(1 - P^k(t)\right) \cdot \frac{MSS}{RTT^k} \cdot \lambda_i^k(t) - P^k(t) \cdot (\lambda_i^k(t))^2 + P^k(t) \cdot MSS \cdot \lambda_i^k(t); \\ \text{режим congestion avoidance} \\ \left(1 - P^k(t)\right) \cdot \left(\frac{MSS}{8 \cdot RTT^k} \cdot \lambda_i^k(t) + \frac{MSS^2}{(RTT^k)^2}\right) - P^k(t) \cdot \left(\lambda_i^k(t)\right)^2 + \\ +P^k(t) \cdot MSS \cdot \lambda_i^k(t) \; k = \overline{(1;K)} \end{cases} \quad (2.1)$$

де $\lambda_i^k(t)$ - інтенсивність трафіку і-го TCP-сеансу з k-м класом обслуговукання, $i = \overline{(1; M^k)}$;

M^k - кількість TCP-сеансів в k-му потоці, $k = \overline{(1; K)}$;

K - кількість класів обслуговування;

RTT^k - час обігу пакетів k-го потоку;

$P^k(t)$ - ймовірність відкидання (блокування) пакетів з k-м класом обслуговування.

Імовірність відкидання пакетів може бути визначена у відповідності з AQM-алгоритмами[20], які реалізують превентивне обмеження черги до її фактичного переповнення. При цьому для кожного класу обслуговування в загальному випадку передбачається організація окремої черги з різними моделями відкидання пакетів. Так для алгоритму довільного раннього виявлення перевантаження RED, який дав розвиток Weighted RED з урахуванням класів обслуговування, розрахунок ймовірності відкидання пакетів з k-м класом обслуговування проводиться відповідно до виразу[23]:

$$P^k(t) = \frac{1}{m^k} \cdot \frac{N^k(t) - N^k_{min}}{N^k_{max} - N^k_{min}} \quad (2.2)$$

де m^k - знаменник граничної ймовірності;

N^k_{max}, N^k_{min} - мінімальний і максимальний розмір черги відповідно;

$N^k(t)$ - середній розмір черги на мережевому вузлі.

Для алгоритму випадкової експоненційної маркування REM вираз для ймовірності P має наступний вигляд:

$$P = 1 - \phi^{-\sum_l p_l(t)} \quad (2.3)$$

де $\phi > 1$ - константа;

$p_l(t)$ - міра переповнення (вартість) в l-му каналі, яка визначається на підставі невідповідності швидкості надходить в канал трафіку і пропускною спроможністю цього каналу, а також різниці між поточним розміром черги і граничним його значенням.

Для подальших досліджень в якості моделі відкидання пакетів використовувався вираз (2.2), а середній розмір черги $N^k(t)$ розраховується за допомогою формули Літтла:

$$N^k(t) = \frac{\sum_{i=1}^{M^k} \lambda_i^k(t)}{B^k - \sum_{i=1}^{M^k} \lambda_i^k(t)} \quad (2.4)$$

де B^k - пропускна здатність, виділена k -му потоку.

З метою підтвердження відповідності запропонованої моделі (2.1) - (2.2) процесу передачі даних в реальних умовах сенсів було досліджено один TCP-сеанс, в ході якого обчислювалася інтенсивність $\lambda_i^k(t)$. В якості вихідних даних виступали величини:

- пропускна здатність каналу B = 100 Мбіт/с;
- вікно прийому на вузлі-одержувачі 64 кбайт;
- розмір сегменту даних MSS = 1460 байт.

Рішення рівнянь (2.1) - (2.2) у ПЗ Mathcad при змінних значеннях RTT зображено на рис 2.8.

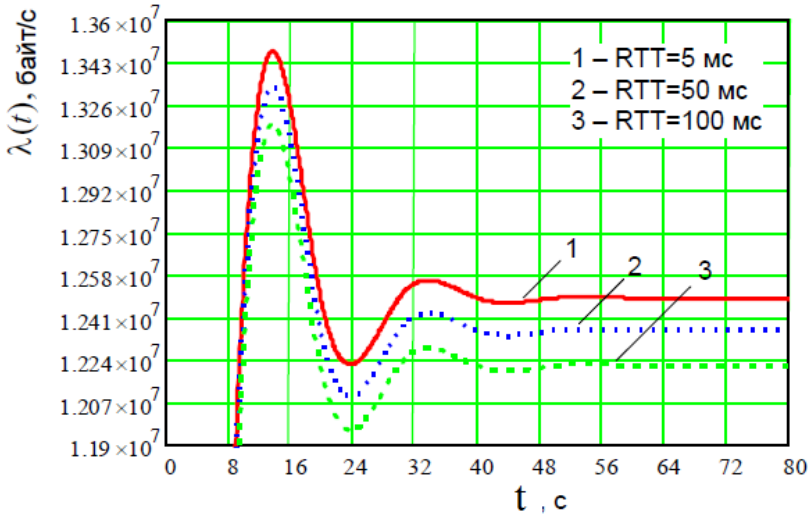


Рисунок 2.8 Зміна інтенсивності передачі даних в TCP-сеансу при різних значеннях RTT

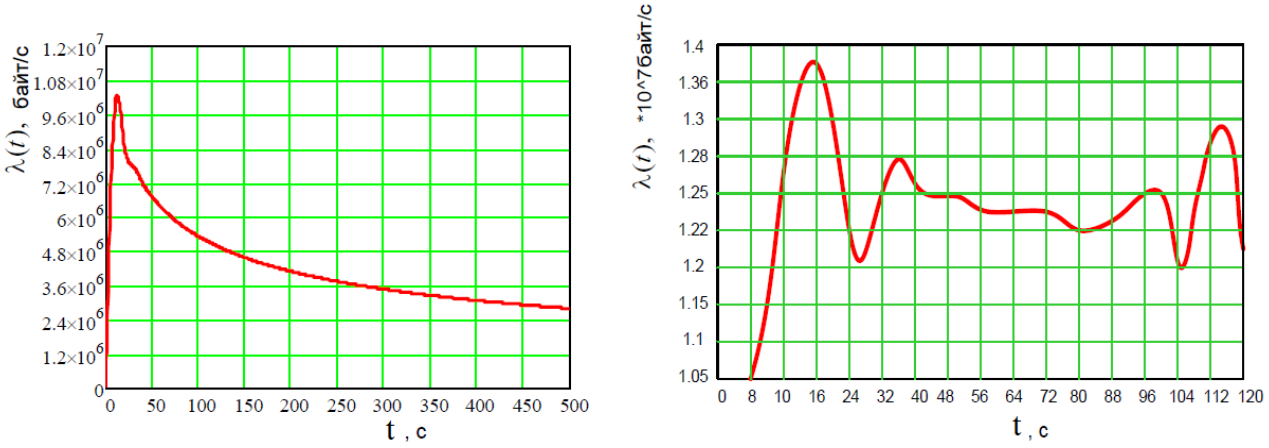
З рис. 2.8 видно, що, по-перше, зміна швидкості передачі (t) носить коливальний характер і в певний момент часу встановлюється на певному значенні, що відповідає реальному процесу інформаційного обміну при роботі протоколу TCP. По-друге, зі зменшенням часу обороту сегмента RTT, від чого залежить поліпшення каналу або вільних канальних і буферних ресурсів. Інтенсивність, яку досягає потік в сталому режимі, зростає і наближається до значення пропускної здатності з'єднання.

Отримана модель (2.1) - (2.2) має чітко виражений нелінійний характер, що з математичної точки зору означає можливу наявність неєдиного рішення системи рівнянь, які є нестійкими і призводять до якісних змін поведінки системи в тих чи інших умовах.

Як показав аналіз, до втрати стійкості призводить коливання як зовнішніх, так і внутрішніх параметрів і умов функціонування. До внутрішніх відносяться параметри протоколу TCP, AQM-алгоритмів і режими передачі відповідно до версії TCP[23]. До зовнішніх параметрів, які призводять до нестійкості сеансу, відносяться зміна структури мережі, наприклад вихід з ладу або додавання мережевих каналів і вузлів, що тягне за собою зміну доступної пропускної здатності, стрибкоподібна зміна інтенсивності переданого трафіку, збільшення затримок поширення, а також присутність інших типів тарфіку.

Дослідження реакції TCP-сеансу на коливання або адміністративні зміни зазначених параметрів і подальшої поведінки здійснюється шляхом внесення змін у вихідну систему рівнянь (2.1) - (2.2). Зміни стосуються або параметрів, що входять до складу системи рівнянь (2.1) - (2.2), або самої структури і виду вихідних диференціальних рівнянь.

На рис 2.9 наведені випадки втрати стійкості, під якою мається на увазі відхилення TCP-сеансу від стаціонарного стану. В даному випадку стаціонарним станом є режим, коли інтенсивність TCP-потоку з часом встановлюється на значенні, близькому до реальної пропускної здатності з'єднання.



a) b)

Рисунок 2.9 Зміна інтенсивності передачі даних при нестійкому TCP-сеансу

Таким чином, варто наголосити на необхідності вирішення такого завдання, як виявлення і аналіз причин і наслідків нестійкого функціонування TCP-сеансів. Ці дослідження дозволять ще на етапі математичного опису ТКС, яке згодом буде основою для перспективних мережних протоколів і технологій, уникнути непередбачених випадків розриву сеансів, зростання затримок, перевантажень мережевих пристроїв і каналів, а, отже, і втрат пакетів.

Проведений аналіз постановки і рішення задачі дослідження стійкості динамічних систем, до яких відноситься TCP-сеанс, представлених нелінійними диференціальними рівняннями, свідчить про доцільність використання теорії біфуркацій та теорії катастроф. Особливостями застосування цих теорій є можливість проаналізувати динаміку поведінки процесів як за допомогою аналітичних виразів, так і за допомогою графічного представлення.

Можливості теорії біфуркацій та теорії катастроф дозволяють обчислити всі рівноважні стану вихідної системи і проаналізувати вплив коливання внутрішніх і зовнішніх параметрів на можливість стрибкоподібного переходу в той чи інший стан, яке може бути як стійким, так і нестійким. Причому з урахуванням особливостей процесів, які протікають в мережі і проявляються в постійних коливаннях таких параметрів як пропускна здатність, інтенсивності потоків трафіків, структури мережі, така можливість є важливою, бо дозволяє вирішити

задачу не тільки аналізу впливу цих коливань на поведінку мережі, а й синтезу, тобто вибору структурних і функціональних параметрів мережі з урахуванням умов стійкості. Рішення такого завдання дозволить уникнути випадків втрати стійкості, тобто невиправданих перевантажень мережі і пов'язаних з цим втрат пакетів.

Однак найбільш адекватним для аналізу стійкості є математичний апарат теорії біфуркацій, оскільки він грунтується на моделях, що описуються диференціальними рівняннями, і не вимагає необхідності побудови специфічних функцій, як у випадках застосування методів Ляпунова і теорії катастроф. В рамках даної теорії забезпечується безпосередній облік параметрів і змінних на рівні математичного опису вихідної динамічної моделі.

Використання математичного апарату теорії біфуркацій для вирішення вихідної задачі аналізу і формулювання умов забезпечення стійкості системи TCP-сеансів (2.1), передбачає таку послідовність дій[23]:

1. Пошук стаціонарних станів системи диференціальних рівнянь.

2. Формування матриці Якобі і розкладання вихідних рівнянь в ряд Тейлора.

3. Отримання системи однорідних лінійних диференціальних рівнянь.

4. Вивід характеристичного рівняння і знаходження його коренів і власних векторів.

5. Побудова траєкторії станів системи (фазового простору) і аналіз поведінки системи в околицях стаціонарних станів. При цьому вид траєкторій станів системи в околиці стаціонарної точки (стійкий нестійкий вузол, сідло і т.д.) визначається коренем характеристичного рівняння.

Виходячи зі значень коренів характеристичного рівняння, формулюються наступні умови забезпечення стійкості TCP-сеансів:

1) для рівноважного стану типу стійкого вузла (рис. 2.10):

$$p_1(\lambda, B, N_{max}) \neq p_2, p_1(\lambda, B, N_{max}) < 0, p_2(\lambda, B, N_{max}) < 0 \qquad (2.5)$$

2) для рівноважного стану типу стійкого фокусу (рис. 2.11):

$$p_1(\lambda, B, N_{max}) = \alpha \pm i\beta, \alpha > 0 \qquad (2.6)$$

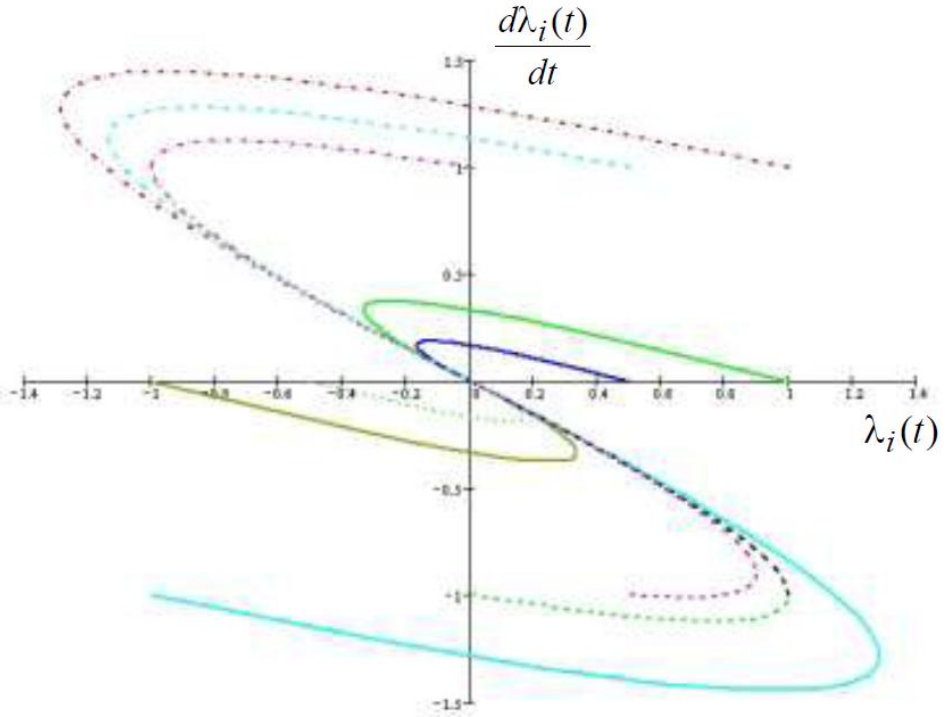


Рисунок 2.10 Фазовий портрет системи TCP-сеансів: рівноважна точка типу стійкий вузол

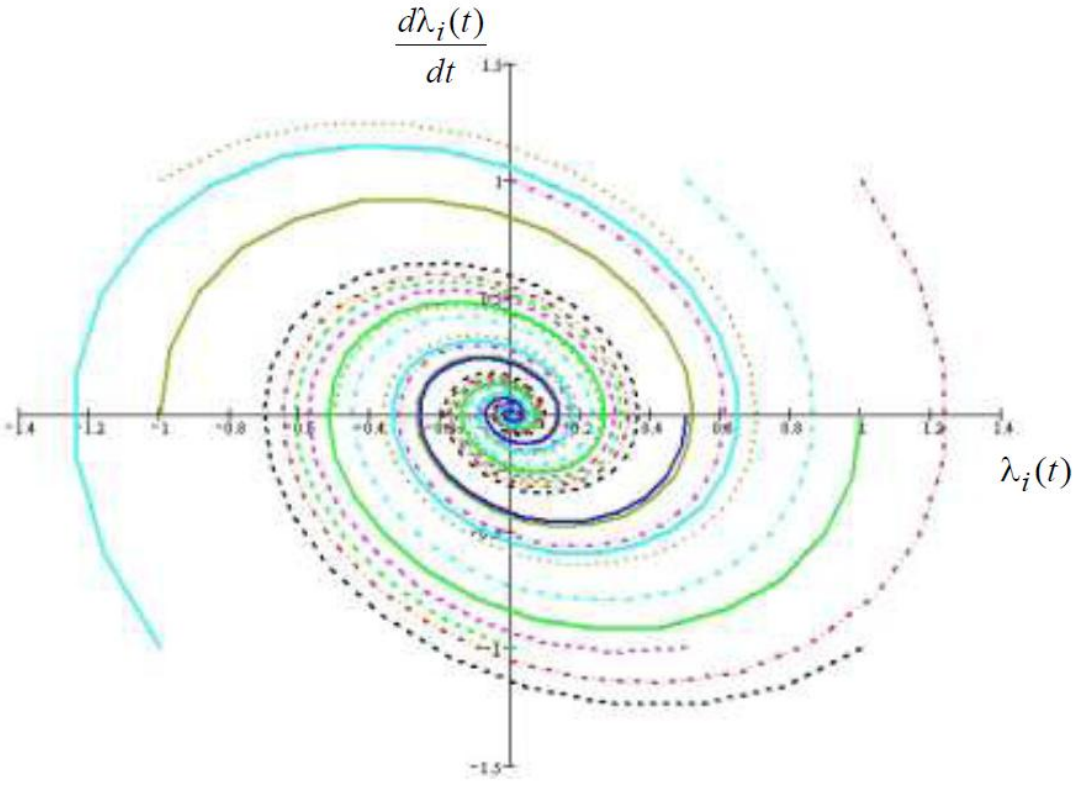


Рисунок 2.11 Фазовий портрет системи TCP-сеансів: рівноважна точка типу стійкий фокус

Таким чином, запропонований метод аналізу стійкості дозволив досліджувати динамічну модель TCP-сеансів, представлену системою нелінійних диференціальних рівнянь (2.1). В ході вирішення цього завдання в аналітичному вигляді були отримані умови забезпечення стійкості TCP-сеансів (2.5) - (2.6), які представлені геометрично в фазопараметричному просторі на рисунках. 2.10 і 2.11. Причому на характер впливають структурні і функціональні параметри мережі (параметри TCP/AQM-алгоритмів, покладених в основу вихідної моделі (2.1) - (2.2), а також топологія мережі, коливання інтенсивності переданого трафіку, багатопотоковості).

Отримані умови забезпечення стійкості TCP-сеансів можуть бути використані з метою вирішення завдання вибору параметрів TCP/AQM-алгоритмів в ході подальшої оптимізації TCP-сеансів.

2.3 Висновки з розділу 2

Для реалізації поставленої задачі по підвищенню якості *IP*-телефонії необхідно впроваджувати в IP-мережах технології по класифікації мережевого трафіку та управління мережевим трафіком.

Засоби управління мережевим трафіком можна позділити:

- маршрутизація;
- вибір протоколу транспортного рівня
- технології управління чергами;
- профілювання трафіку.

РОЗДІЛ 3. ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ АЛГОРИТМІВ ПРІОРІТИЗАЦІЇ ДЛЯ ПЕРЕДАЧІ МУЛЬТИСЕВІСНОГО ТРАФІКУ

3.1. Початкові данні для проведення експериментального дослідження

3.1.1 Генератор трафіка D-ITG

Пакет для тестування проходження трафіку D-ITG має широкі функціональні можливості, наприклад здатність генерувати трафік з такими видами розподілу як рівномірне, експоненціальне, Парето, Коші та інші, що дозволяє оцінювати значення основних показників QoS. Програмне забезпечення складається з підпрограм[26]:

D-ITG Sender - для відправки пакетів(рис.3.1);

D-ITGReceiver - для отримання пакетів(рис.3.2);

D-ITGDecoder - для декодування та аналізу файлів журналів, що створюються в ITGSender та ITGReceiver, і обчислює середні значення бітрейту, затримки та джиттера на певних інтервалах експерименту (рис.3.2).

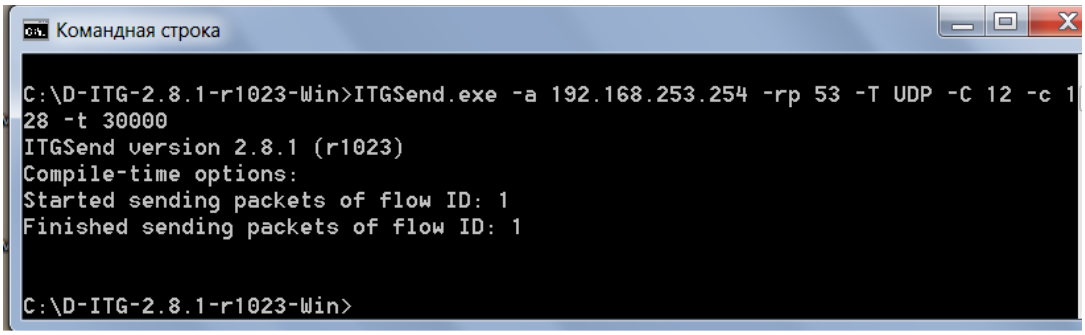


Рисунок 3.1 Приклад генерації трафіку з використанням програмного забезпечення D-ITG Sender

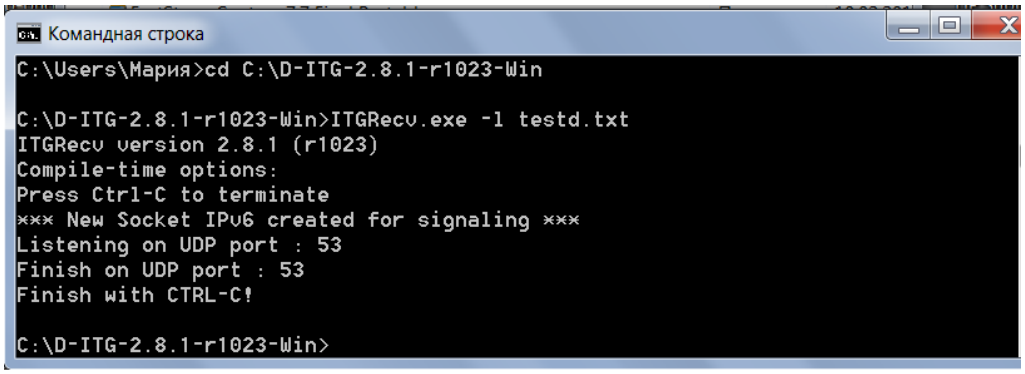


Рисунок. 3.2 Приклад прийому трафіку з використанням програмного забезпечення D-ITG Receiver

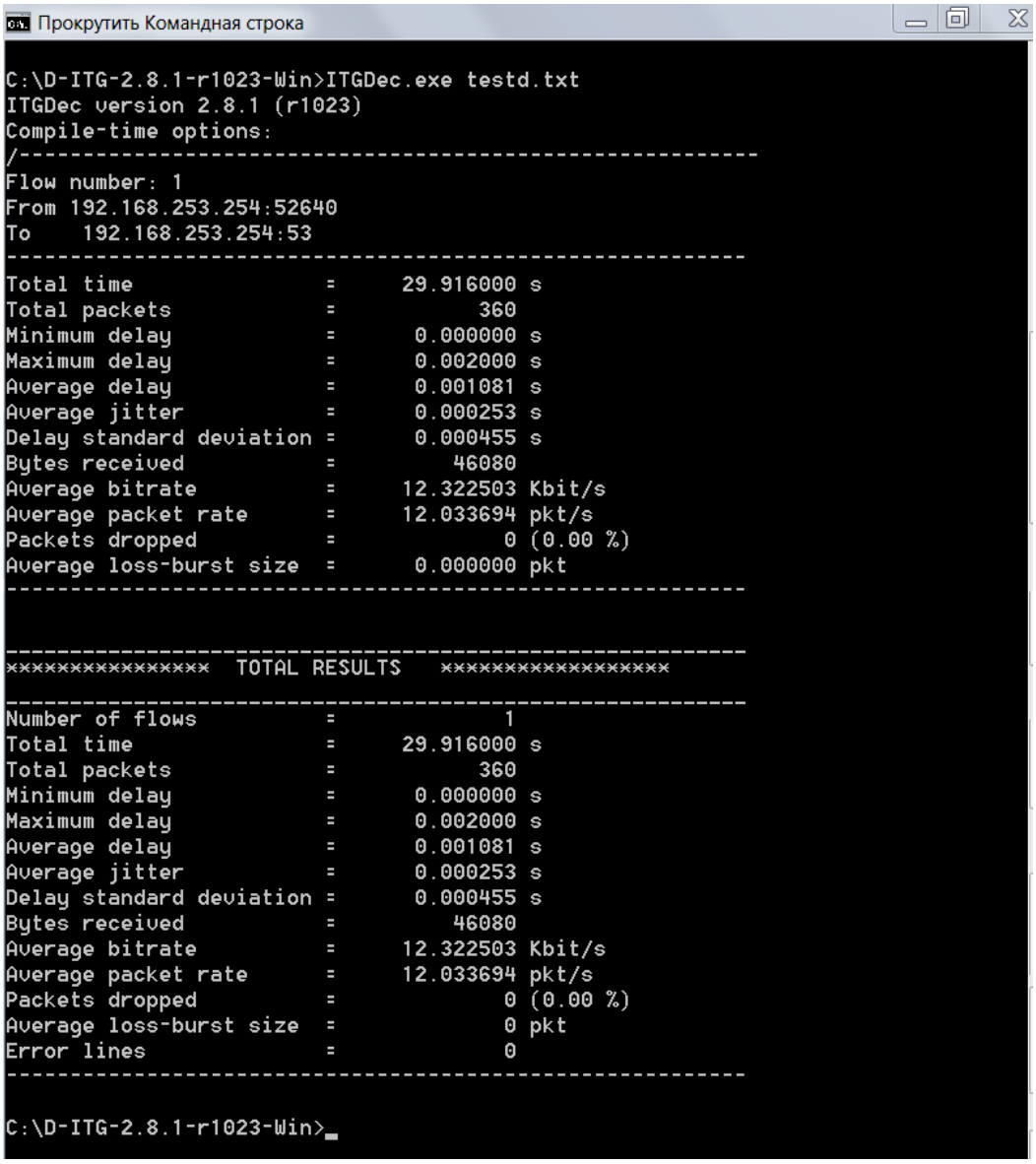


Рисунок 3.3 Приклад виводу показників якості з використанням програмного забезпечення D-ITG Decoder

На рисунку 3.4. представлені параметри, які можливо задавати при відправці з D-ITG Sender[27].

ITGSend [**–m** ⟨msr_type⟩] [**–a** ⟨destination_address⟩] [**–rp** ⟨destination_port⟩] [**–sp** ⟨source_port⟩] [**–T** ⟨protocol_type⟩] [**–f** ⟨TTL⟩] [**–b** ⟨DS byte⟩] [**–rk** ⟨receiver_serial_iface⟩] [**–sk** ⟨sender_serial_iface⟩] [**–D**] [**–P**] [**–s** ⟨seed⟩] [**–t** ⟨duration⟩] [**–d** ⟨gen_delay⟩] [**–p** ⟨payload_log_type⟩] [**–j** ⟨enable_idt_recovery⟩] [**–l** [⟨logfile⟩]] [**–L** [⟨log_server_addr⟩] [⟨protocol_type⟩]] [**–x** [⟨receiver_logfile⟩]] [**–X** [⟨log_server_addr⟩] [⟨protocol_type⟩]] [[**–C** ⟨pkts_per_s⟩ | **–U** ⟨min_pkts_per_s⟩⟨max_pkts_per_s⟩ | **–E** ⟨average_pkts_per_s⟩ | **–V** ⟨shape⟩⟨scale⟩ | **–Y** ⟨shape⟩⟨scale⟩ | **–N** ⟨mean⟩⟨std_dev⟩ | **–O** ⟨average_pkts_per_s⟩ | **–G** ⟨shape⟩⟨scale⟩] [**–c** ⟨pkt_size⟩ | **–u** ⟨min_pkt_size⟩⟨max_pkt_size⟩ | **–e** ⟨average_pkt_size⟩ | **–v** ⟨shape⟩⟨scale⟩ | **–y** ⟨shape⟩⟨scale⟩ | **–n** ⟨mean⟩⟨std_dev⟩ | **–o** ⟨average_pkt_size⟩ | **–g** ⟨shape⟩⟨scale⟩]] | [**Telnet** | **DNS** | **CSa** | **CSi** | **Quake3** | **VoIP** [**–x** ⟨codec_type⟩] [**–h** ⟨protocol_type⟩] [**–VAD**]]

Рисунок 3.4 Параметри в D-ITG Sender

Також при виборі змінного розміру пакету можна задати закон розподілу. На рисунку 3.5. показані закони розподілу розмірів пакетів[27].

Inter-departure time options:

–C ⟨pkts_per_s⟩	Constant inter-departure time (IDT)
–U ⟨min_pkts_per_s⟩ ⟨max_pkts_per_s⟩	Uniformly distributed IDT
–E ⟨average_pkts_per_s⟩	Exponentially distributed IDT
–V ⟨shape⟩ ⟨scale⟩	Pareto distributed IDT
–Y ⟨shape⟩ ⟨scale⟩	Cauchy distributed IDT
–N ⟨mean⟩ ⟨std_dev⟩	Normal distributed IDT
–O ⟨average_pkts_per_s⟩	Poisson distributed IDT
–G ⟨shape⟩ ⟨scale⟩	Gamma distributed IDT

Рисунок 3.5 Закони розподілення розмірів пакетів

Результати заносяться до бінарного файлу, який на рисунку 3.2 вказаний як testd.txt. Далі за допомогою D-ITGDecoder на основі отриманого testd.txt отримуємо текстові масиви даних з основними показникам якості обслуговування. Параметри, які можна задати для D-ITGDecoder описані вище на рисунку 3.3.

3.1.2 Топологія експериментальної установки. Налаштування обладнання

Для проведення експериментального дослідження та зборки експериментальної установки було взято:

- два маршрутизатора Cisco 2600 під управлінням ОС IOS 12.4;
- два ноутбука з ОС Windiws 10 зі вставленим програмним забезпеченням для генерації та аналізу мережевого трафіка D-ITG.

На рис. 3.6 показана топологія для проведення експерименту.

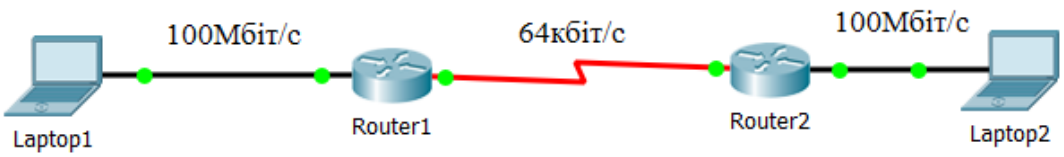


Рисунок 3.6 Топологія експериментальної установки

Налаштування ноутбуків та маршрутизаторів описані нижче.

На Laptop1 була налаштована IP-адреса 10.10.1.2 з маскою 255.255.255.0 та IP-адресою шлюзу 10.10.1.1. Так як з Laptop1 - відправник, на ньому був встановлений D-ITG Sender для генерації трафіку.

На Laptop2 була налаштована IP-адреса 10.10.2.2 з маскою 255.255.255.0 та IP-адресою шлюзу 10.10.2.1. На приймальній стороні був встановлений D-ITG Receiver для прослуховування і запису в текстовий файл отриманих пакетів, які генерує Laptop1.

На маршрутизаторі Router1 на серіальному інтерфейсі S0/0 була налаштована IP-адреса 10.10.10.1 з маскою 255.255.255.252 також була встановлена пропускна спроможність 64 кбіт/сек для проведення дослідження по пріорітизації трафіку. На інтерфейсі Fastethernet0/0 була налаштована IP-адреса 10.10.1.1 з маскою підмережі 255.255.255.0.

На маршрутизаторі Router2 на послідовному інтерфейсі S0/1 була назначена IP-адреса 10.10.10.2 з маскою 255.255.255.252. На інтерфейсі Fastethernet0/0 була налаштована IP-адресса 10.10.2.1 з маскою підмережі 255.255.255.0. На маршрутизаторах Router1, Router2 була налаштована статична маршрутизація за допомогою команд на рисунку 3.7.[28]

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
Router2(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

Рисунок 3.7 Налаштування статичної маршрутизації

В експериментальному дослідженні за допомогою генератора трафіку D-ITG на комп'ютері Laptop1 генерується трафік від 4х мережевих додатків:

- IP-телефонія (порт 17001);
- SMTP - електрона пошта (порт 25);
- DNS - запити служби домених імен (порт 53);
- HTTP - веб-трафік (порт 80).

Для відправки трафіку 4-ма потоками одночасно був заданий скрипт, який показаний на рисунку 3.5, де 10.10.2.2 - адреса вузла отримувача, UDP - протокол транспортного рівня, 5 - кількість пакетів за секунду, 128біт - розмір пакетів, 30000мілісекунд=30секунд - це час генерації трафіку. Надалі буде змінюватися саме кількість згенерованих пакетів за секунду.

```
1  -a 10.10.2.2 -rp 17001 -T UDP -C 5 -c 128 -t 30000
2  -a 10.10.2.2 -rp 25    -T UDP -C 5 -c 128 -t 30000
3  -a 10.10.2.2 -rp 53    -T UDP -C 5 -c 128 -t 30000
4  -a 10.10.2.2 -rp 80    -T UDP -C 5 -c 128 -t 30000
5
```

Рисунок3.8 Batch-скрипт для генерації мультисервісного трафіку при значенні бітрейту 20 кбіт/сек

У першому випадку за генеруємо мережевий трафік з сумарним бітрейтом всіх потоків 20 кбіт/сек, який проходить від Laptop1 до Laptop2. Бітрейт згенерованого трафіка суттєво нижчий ніж пропускна спроможність каналу 64 кбіт/сек, який був налаштований між маршрутизаторами. За допомогою програмного забезпечення D-ITG одночасно генеруємо чотири типи трафіку з характеристивами, які були задані в скрипті на рисунку 3.8.

У другому випадку за генеруємо мережевий трафік сумарним бітрейтом всіх потоків 61 кбіт/сек, який проходить від Laptop1 до Laptop2. Бітрейт трафіка наближається до значення пропускної спроможності 64 кбіт/сек. За допомогою програмного забезпечення D-ITG одночасно генеруємо чорири типи трафіку з характеристивами, які були задані в скрипті на рисунку 3.9.

```
-a 10.10.2.2 -rp 17001 -T UDP -C 15 -c 128 -t 30000
-a 10.10.2.2 -rp 25    -T UDP -C 15 -c 128 -t 30000
-a 10.10.2.2 -rp 53    -T UDP -C 15 -c 128 -t 30000
-a 10.10.2.2 -rp 80    -T UDP -C 15 -c 128 -t 30000

```

Рисунок 3.9 Batch-скрипт для генерації мультисервісного трафіку при значенні бітрейту 61 кбіт/сек

У третьому випадку генеруємо мережевий трафік (70 кбіт/сек, який проходить від Laptop1 до Laptop2. Бітрейт трафіка вже перевищує значення пропускної спроможності 64 кбіт/сек. За допомогою програмного забезпечення D-ITG одночасно генеруємо чорири типи трафіку з характеристивами, які були задані в скрипті на рисунку 3.10.

```
-a 10.10.2.2 -rp 17001 -T UDP -C 17 -c 128 -t 30000
-a 10.10.2.2 -rp 25    -T UDP -C 17 -c 128 -t 30000
-a 10.10.2.2 -rp 53    -T UDP -C 17 -c 128 -t 30000
-a 10.10.2.2 -rp 80    -T UDP -C 17 -c 128 -t 30000

```

Рисунок 3.10 Batch-скрипт для генерації мультисервісного трафіку при значенні бітрейту 70 кбіт/сек

У четвертому випадку генеруємо мережевий трафік (78 кбіт/сек, який проходить від Laptop1 до Laptop2. Бітрейт трафіка перевищує значення пропускної спроможності 64 кбіт/сек. За допомогою програмного забезпечення D-ITG одночасно генеруємо чорири типи трафіку з характеристивами, які були задані в скрипті на рисунку 3.11.

```
1  -a 10.10.2.2 -rp 17001 -T UDP -C 19 -c 128 -t 30000
2  -a 10.10.2.2 -rp 25    -T UDP -C 19 -c 128 -t 30000
3  -a 10.10.2.2 -rp 53    -T UDP -C 19 -c 128 -t 30000
4  -a 10.10.2.2 -rp 80    -T UDP -C 19 -c 128 -t 30000
5
```

Рисунок 3.11 Batch-скрипт для генерації мультисервісного трафіку при значенні бітрейту 78 кбіт/сек

У п'ятому випадку генеруємо мережевий трафік (98 кбіт/сек, який проходить від Laptop1 до Laptop2. Бітрейт трафіка значно перевищує значення пропускної спроможності 64 кбіт/сек. За допомогою програмного забезпечення D-ITG одночасно генеруємо чорири типи трафіку з характеристивами, які були задані в скрипті на рисунку 3.12.

```
1  -a 10.10.2.2 -rp 17001 -T UDP -C 24 -c 128 -t 30000
2  -a 10.10.2.2 -rp 25    -T UDP -C 24 -c 128 -t 30000
3  -a 10.10.2.2 -rp 53    -T UDP -C 24 -c 128 -t 30000
4  -a 10.10.2.2 -rp 80    -T UDP -C 24 -c 128 -t 30000
5
```

Рисунок 3.12 Batch-скрипт для генерації мультисервісного трафіку при значенні бітрейту 98 кбіт/сек

3.2 Етапи проведення експерименту

Для вирішення задачі підвищення якості IP-телефонії важливо контролювати показники мережі при передачі мережевого трафіку, які наведені в таблиці 3.2.

Таблиця 3.2 Показники, які використовуються при проведенні дослідження

Показник	Опис	Одиниця вимірювання
Втрата пакетів	Описує, яка кількість пакетів втрачається при передаванні від вузла відправника до вузла отримувуча	%
Бітрейт	Описує, який об’єм трафіку передається в секунду	кбіт/сек
Затримка	Описує час за який пакет потрапляє від вузла відправника до вузла отримувача	мілісекунда
Джитер	Описує різницю в затримці при передачі пакетів одного потоку	мілісекунда

3.2.1 Експеримент №1. Дослідження пріорітизації трафіка на основі технології управління чергами FIFO

На маршрутизаторі Router1 була налаштована технологія управління чергами FIFO[26].

```
Router1(config)#interface serial0/0
Router1(config-if)#no fair-queue
```

Рисунок 3.10. Налаштування технології управління чергами FIFO

Після того, як були запущені скрипти, які описані вище в пункті 3.2.2, були зняті і записані результати за допомогою D-ITG Decoder і внесені таблицю 3.3.

Таблиця 3.3 Показники втрати пакетів для чотирьох типів трафіку (FIFO)

Тип трафіку	Втрата пакетів, %				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	0	11,12	26,71	38,33	46,33
SMTP	0	19,86	25,2	36,36	49,62
DNS	0	10,73	26,43	38,87	45,96
HTTP	0	16,27	28,52	36,36	47,18

На рис.3.11. показаний графік залежності втрати пакетів від загальної швидкості генерації трафіку для чотирьох типів трафіку, які використовуються в експеременті.

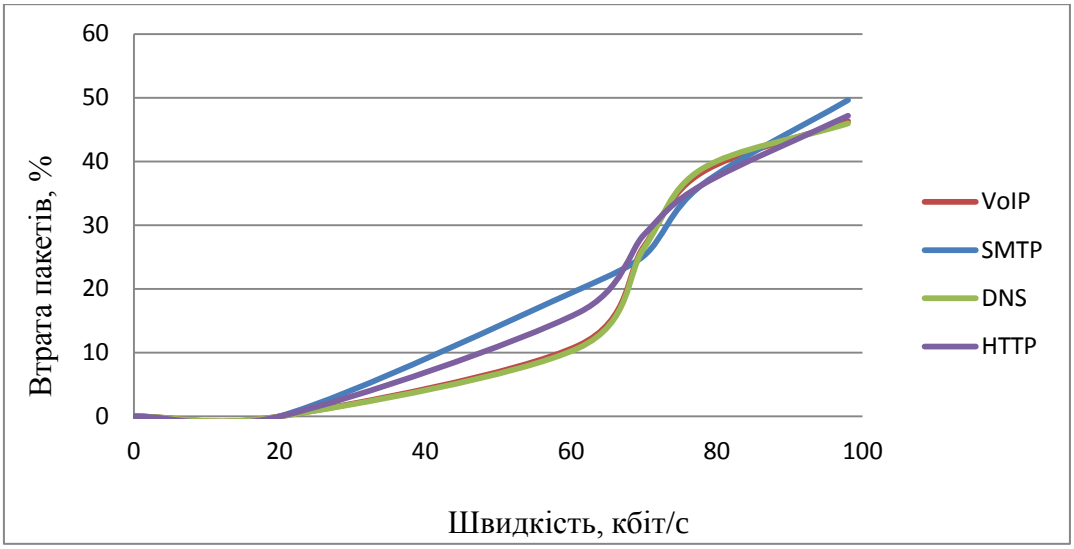


Рисунок 3.11 Графік залежності втрати пакетів для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (FIFO)

В таблиці 3.4 вказані показники бітрейту, для чотирьох типів трафіку, які були зняті при проведенні екпременту.

Таблиця 3.4 Показники бітрейту для чотирьох типів трафіку (FIFO)

Тип трафіку	Бітрейт, кбіт/с				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	5,1	14,3	14,5	15,5	12,5
SMTP	5,1	14,7	13,9	15,9	11,6
DNS	5,1	15,5	13,3	16,3	14,3
HTTP	5,1	14,5	14,2	15,6	14,5

На рис. 3.12 показаний графік залежності бітрейту для чотирьох типів трафіку від загальної швидкості генерації трафіку..

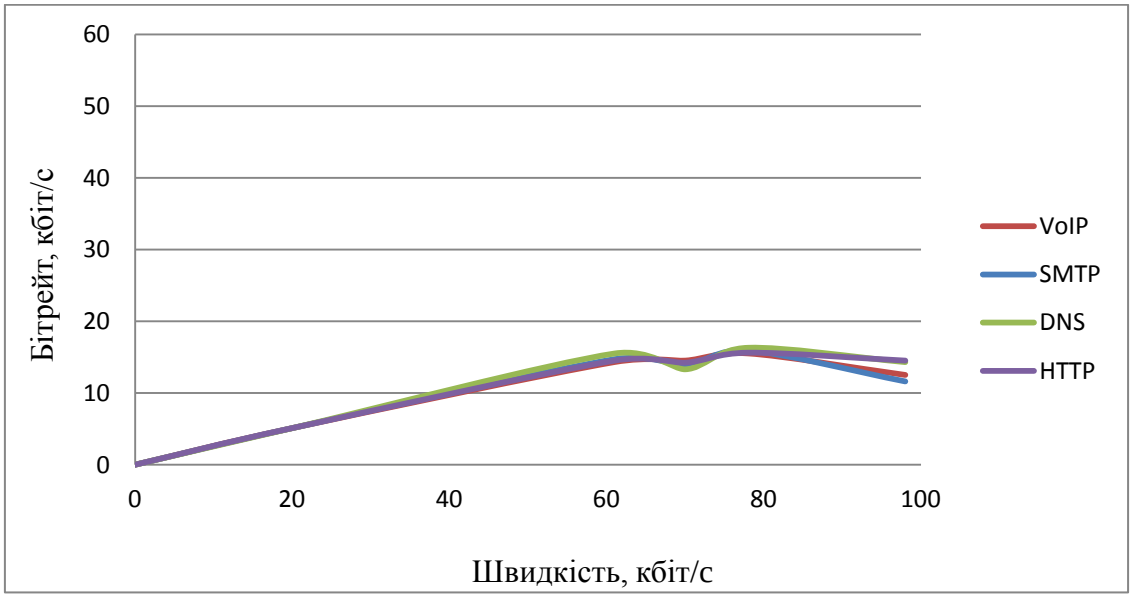


Рисунок 3.12 Графік залежності бітрейту для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (FIFO)

В таблиці 3.5. вказані показники затримки, для чотирьох типів трафіку, які були зняті при проведенні екпременту.

Таблиця 3.5 Показники затримки пакетів для чотирьох типів трафіку (FIFO)

Тип трафіку	Середня затримка, мс				
	№1 (20кбіт/с)	№1 (61кбіт/с)	№1 (70кбіт/с)	№1 (78кбіт/с)	№1 (98кбіт/с)
VoIP	2,24	3,16	8,41	12,63	19,4
SMTP	2,22	3,19	8,26	13,15	18,6
DNS	2,21	3,25	8,38	13,7	19,3
HTTP	2,21	3,32	8,97	13,3	19,4

На рис.3.13. показаний графік залежності затримки для чотирьох типів трафіку від загальної швидкості генерації трафіку.

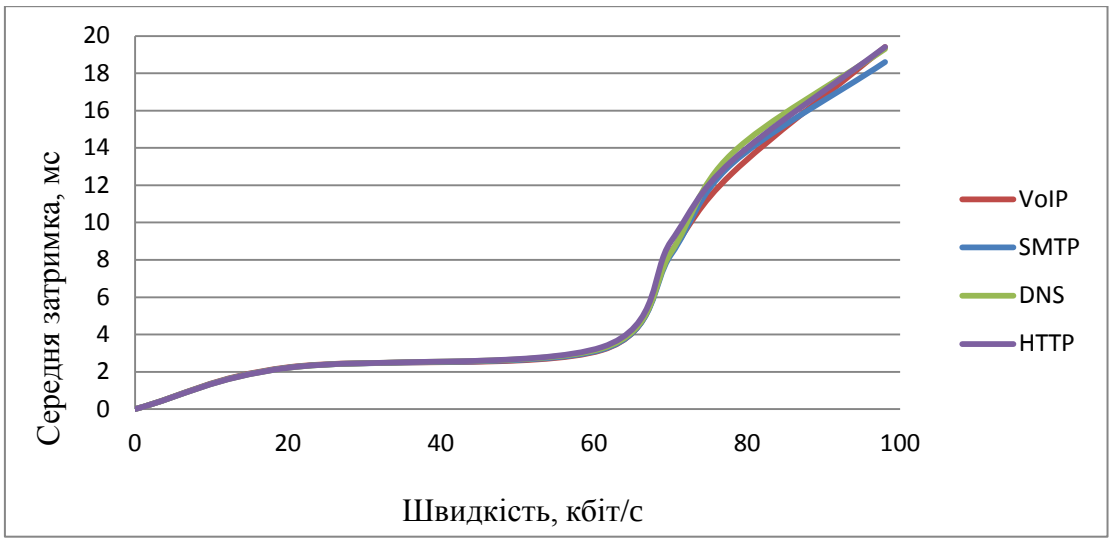


Рисунок 3.13 Графік залежності затримки пакетів для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (FIFO)

В таблиці 3.6. вказані показники варіативності, для чотирьох типів трафіку, які були зняті при проведенні екпременту.

Таблиця 3.6 Показники джитеру для чотирьох типів трафіку (FIFO)

Тип трафіку	Джитер, мс				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	0,009	0,016	0,025	0,037	0,068
SMTP	0,01	0,016	0,023	0,035	0,06
DNS	0,009	0,016	0,026	0,035	0,07
HTTP	0,011	0,015	0,022	0,039	0,075

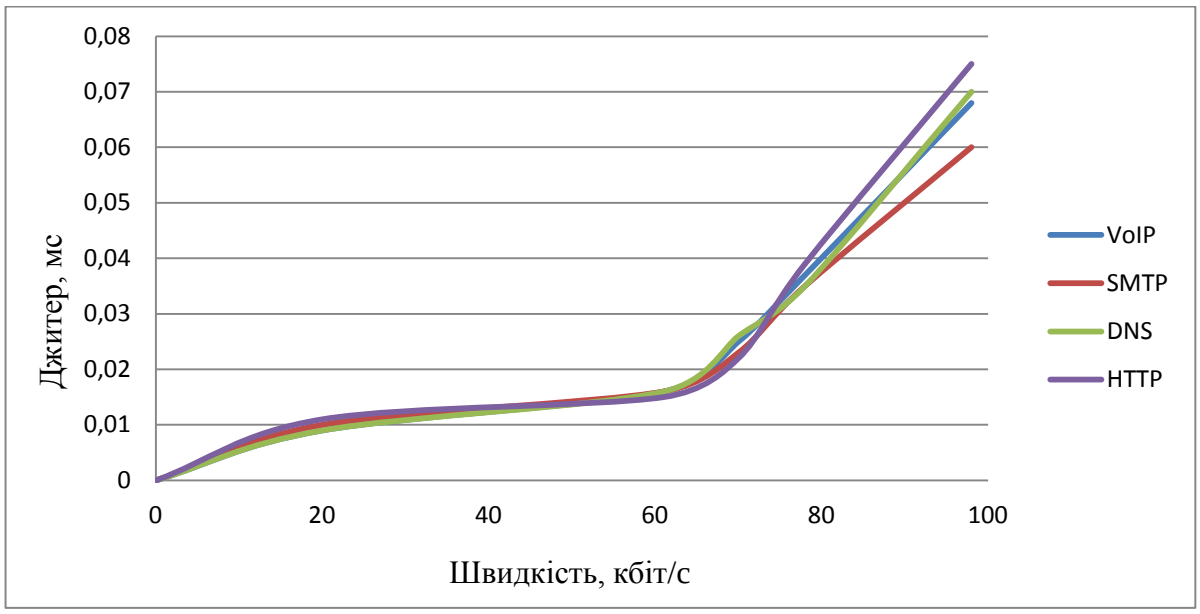


Рисунок 3.14. Графік залежності варіативності для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (FIFO)

3.2.2 Експеримент №2. Дослідження пріорітизації трафіка при використанні технології управління чергами PQ

На маршрутизаторі Router2 була налаштована технологія управління чергами PQ, конфігурація якої представлена на рисунку 3.15.

```
Router1(config)#access-list 101 permit udp any any eq 17001
Router1(config)#access-list 102 permit udp any any eq 25
Router1(config)#access-list 103 permit udp any any eq 53
Router1(config)#access-list 104 permit udp any any eq 80

Router1(config)#priority-list 1 protocol ip high list 101
Router1(config)#priority-list 1 protocol ip medium list 102
Router1(config)#priority-list 1 protocol ip normal list 103
Router1(config)#priority-list 1 protocol ip low list 104

Router1(config)#interface serial0/0
Router1(config-if)#priority-group 1
```

Рисунок 3.16. Налаштування технології управління чергами PQ

Після того, як були запущені скрипти, які описані в пункті 3.2.2, були зняті і записані результати за допомогою D-ITG Decoder і внесені таблицю 3.7.

Таблиця 3.7 Показники втрати пакетів для чотирьох типів трафіку (PQ)

Тип трафіку	Втрата пакетів, %				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	0	0	0	0	0
SMTP	0	0	0	0	3,1
DNS	0	2,7	17,8	37,3	75
HTTP	0	5,8	35,3	51,6	88,1

На рис.3.17. показаний графік залежності втрати пакетів від загальної швидкості генерації трафіку для чотирьох типів трафіку, які використовуються в експерименті.

В таблиці 3.8. вказані показники бітрейту, для чотирьох типів трафіку, які були зняті при проведенні екпременту.

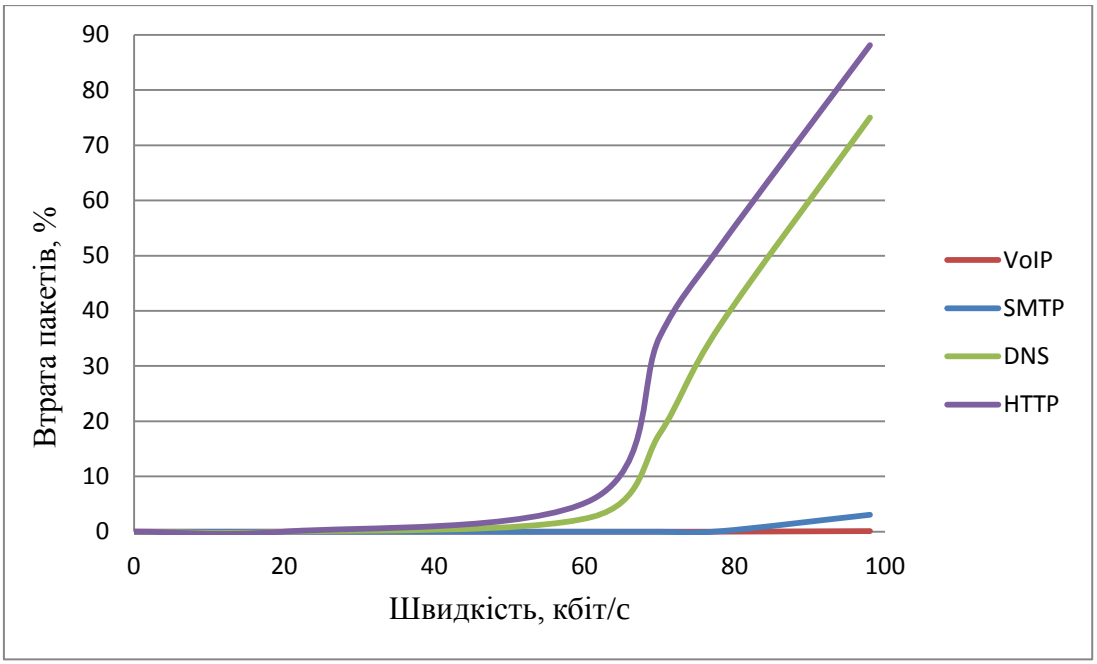


Рисунок 3.17. Графік залежності втрати пакетів для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (PQ)

Табл. 3.8 Показники біт рейту для чотирьох типів трафіку (PQ)

Тип трафіку	Бітрейт, кбіт/с				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	5,2	15,4	17,4	19,5	24,6
SMTP	5,2	15,2	17,3	19,2	22,8
DNS	5,2	14,4	13,8	11,7	2,9
HTTP	5,2	14,2	10,8	7,4	1,2

На рис.3.18. показаний графік залежності бітрейту для чотирьох типів трафіку від загальної швидкості генерації трафіку.

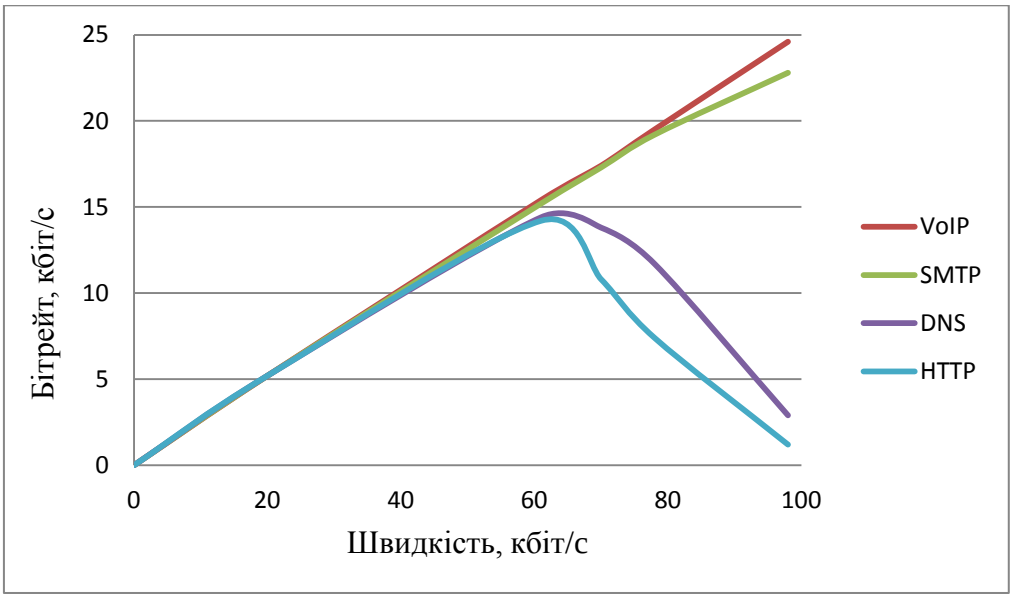


Рисунок 3.18. Графік залежності бітрейту для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (PQ)

В таблиці 3.9 вказані показники затримки, для чотирьох типів трафіку, які були зняті при проведенні екпременту

Таблиця 3.9 Показники середньої затримки пакетів для PQ

Тип трафіку	Середня затримка, мс				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	2,21	2,23	2,36	2,4	2,48
SMTP	2,21	2,27	3,51	4,68	8,27
DNS	2,35	2,83	6,29	14,75	27,1
HTTP	2,35	3,32	11,84	19,3	29,8

На рис.3.19. показаний графік залежності затримки пакетів від загальної швидкості генерації трафіку для чотирьох типів трафіку, які використовуються

в експерименті. В таблиці 3.10. вказані показники варітивності, для чотирьох типів трафіку, які були зняті при проведенні екпременту

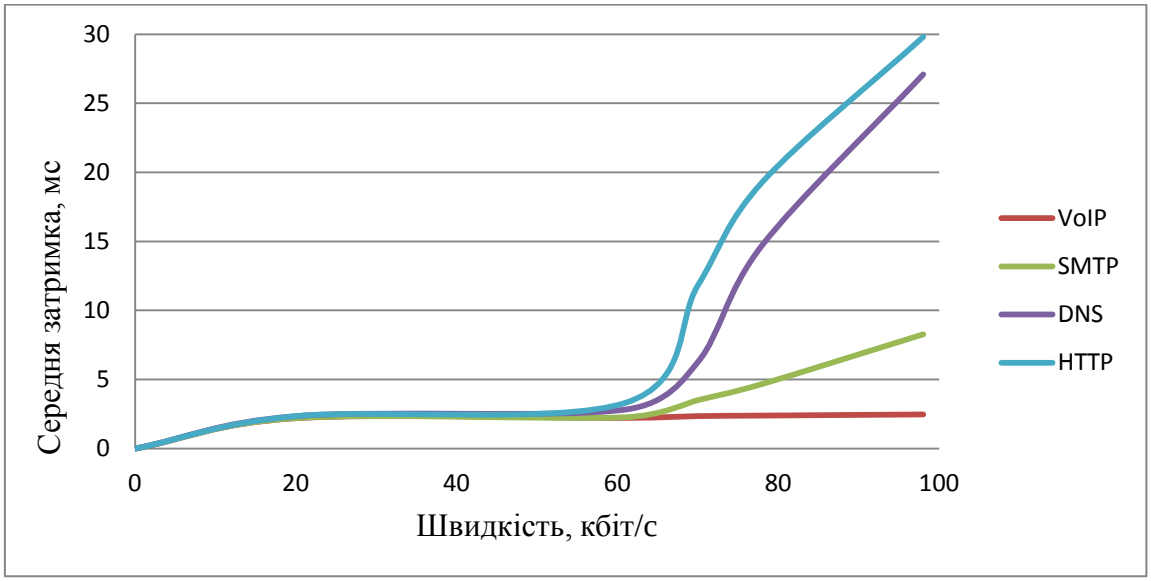


Рисунок 3.19. Графік залежності затримки для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (PQ)

Таблиця 3.10 Показники джитеру для чотирьох типів трафіку (PQ)

Тип трафіку	Джитер, мс				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	0,003	0,007	0,011	0,011	0,01
SMTP	0,004	0,007	0,011	0,027	0,061
DNS	0,005	0,016	0,026	0,035	0,087
HTTP	0,013	0,022	0,032	0,074	0,134

На рис.3.20. показаний графік залежності джитеру від загальної швидкості генерації трафіку для чотирьох типів трафіку, які використовуються в експерименті.

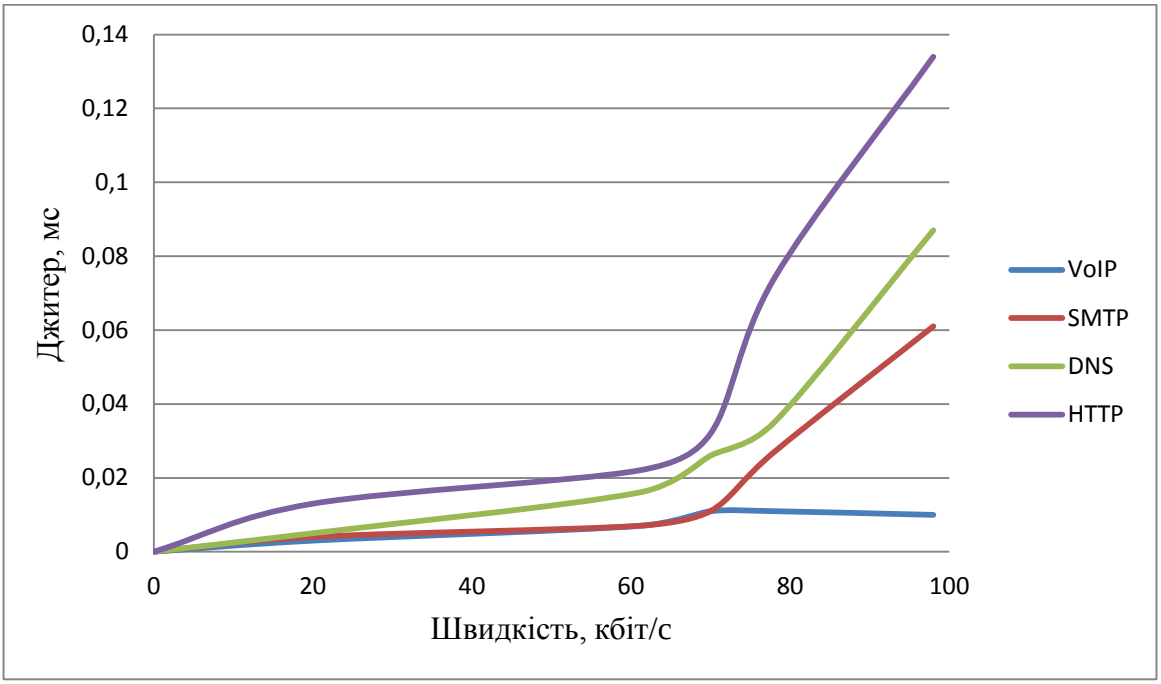


Рисунок 3.20. Графік залежності джитеру для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (PQ)

3.2.3 Експеримент №3. Дослідження пріорітизації трафіка на основі технології управління чергами CQ

Для проведення цього експерименту на інтерфейсі S0/0 (64 кбіт/сек) маршрутизатора Router2 був налаштована технологія управління чергами CQ.

Після того, як були проведені виміри з комп'ютера Laptop2 (на якому D-ITG налаштований в режимі приймання пакетів) були зняти показники втрати пакетів та занесені таблицю 3.11.

На рис.3.22 показаний графік залежності втрати пакетів від загальної швидкості генерації трафіку для чотирьох типів трафіку, які використовуються в експерименті.

```
Router1(config)#access-list 101 permit udp any any eq 17001
Router1(config)#access-list 102 permit udp any any eq 25
Router1(config)#access-list 103 permit udp any any eq 53
Router1(config)#access-list 104 permit udp any any eq 80

Router1(config)#queue-list 2 protocol ip 1 list 101
Router1(config)#queue-list 2 protocol ip 2 list 102
Router1(config)#queue-list 2 protocol ip 3 list 103
Router1(config)#queue-list 2 protocol ip 4 list 104

Router1(config)#queue-list 2 queue 1 byte-count 4000
Router1(config)#queue-list 2 queue 2 byte-count 2000
Router1(config)#queue-list 2 queue 3 byte-count 1000
Router1(config)#queue-list 2 queue 4 byte-count 500

Router1(config)#interface serial0/0
Router1(config-if)#custom-queue-list 2
```

Рисунок 3.21 Налаштування технології управління чергами CQ

Таблиця 3.11 Показники втрати пакетів для чотирьох типів трафіку (CQ)

Тип трафіку	Втрата пакетів, %				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	0	0	0	0	1,6
SMTP	0	0	12,7	21,1	40,9
DNS	0	21,9	40,3	55,7	69,6
HTTP	0	41,6	60,3	73,5	82,6

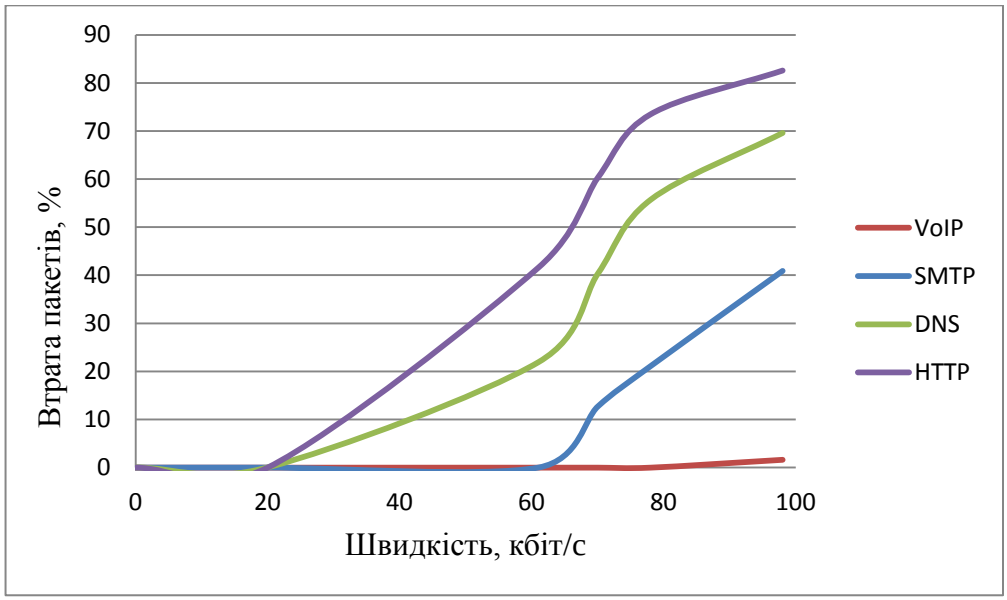


Рисунок 3.22 Графік залежності втрати пакетів для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (CQ)

В таблиці 3.12 вказані показники бітрейту, для чотирьох типів трафіку, які були зняті при проведенні екпременту

Таблиця 3.12 Показники бітрейту для чотирьох типів трафіку (CQ)

Тип трафіку	Бітрейт, кбіт/с				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	5,1	15,2	17,5	19,2	23,1
SMTP	5,1	15,3	14,4	13,1	12,1
DNS	4,9	12	8,3	6,8	6,2
HTTP	4,9	6,4	3,7	3,4	3,1

На рис.3.23 показаний графік залежності бітрейту для чотирьох типів трафіку від загальної швидкості генерації трафіку..

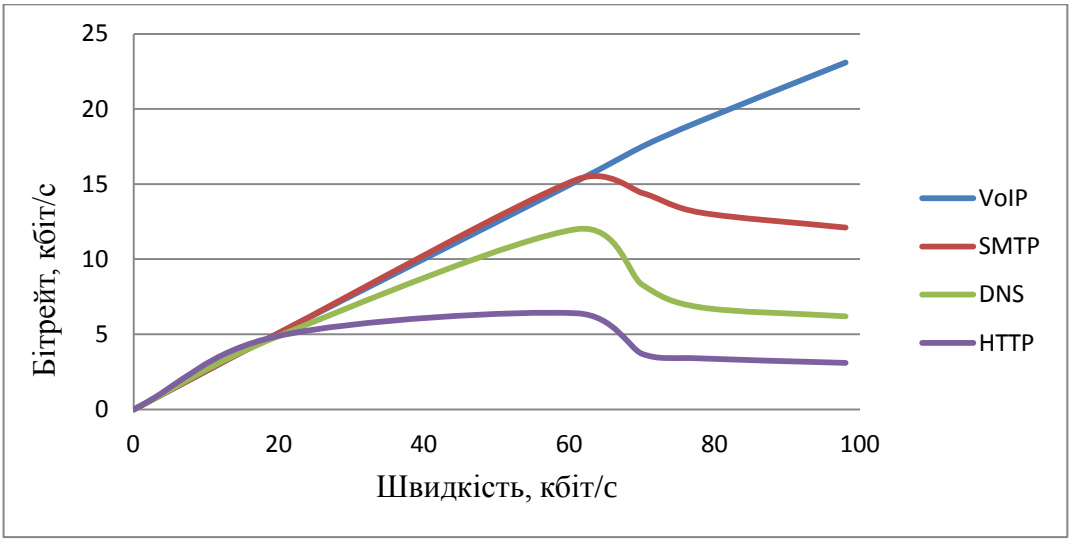


Рисунок 3.23 Графік залежності бітрейту для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (CQ)

В таблиці 3.13. вказані показники затримки, для чотирьох типів трафіку, які були зняті при проведенні екпременту для випадку

Таблиця 3.13 Показники затримки пакетів для чотирьох типів трафіку (CQ)

Тип трафіку	Середня затримка, мс				
	№1 (20кбіт/с)	№1 (61кбіт/с)	№1 (70кбіт/с)	№1 (78кбіт/с)	№1 (98кбіт/с)
VoIP	2,2	2,4	2,44	2,52	2,74
SMTP	2,21	2,45	3,11	4,15	7,96
DNS	2,32	3,16	6,84	14,7	20,3
HTTP	2,32	3,32	10,37	15,3	22,4

На рис. 3.24 показаний графік залежності затримки пакетів від загальної швидкості генерації трафіку для чотирьох типів трафіку.

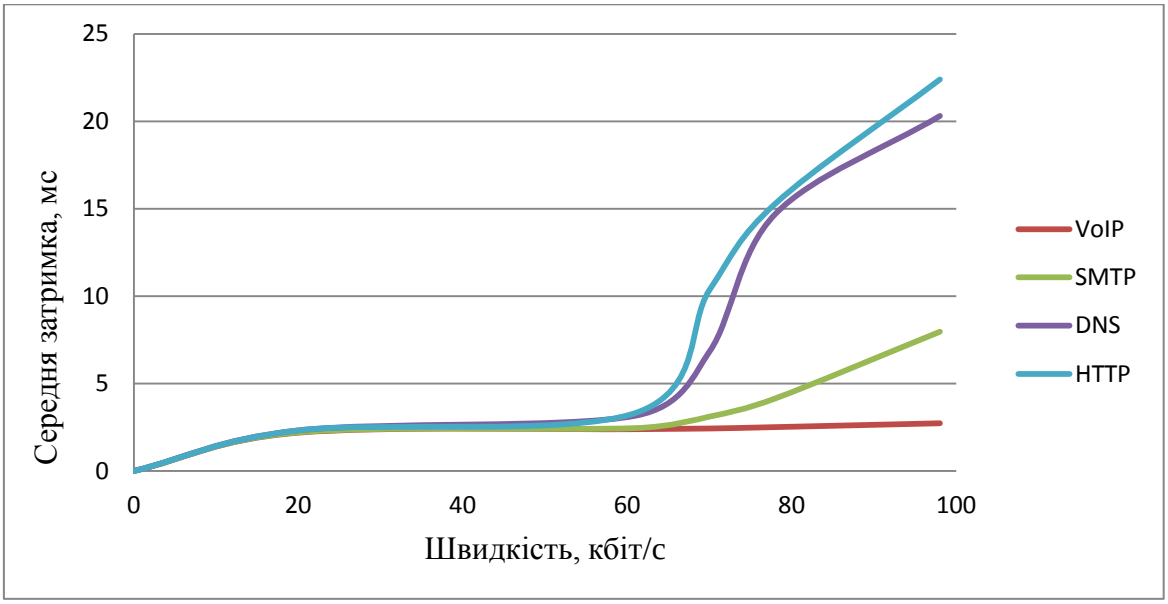


Рисунок 3.24. Графік залежності затримки пакетів для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (CQ)

В таблиці 3.14 вказані показники джитеру, для чотирьох типів трафіку.

Таблиця 3.14 Показники варіативності для чотирьох типів трафіку (CQ)

Тип трафіку	Джитер, мс				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
VoIP	0,003	0,006	0,011	0,012	0,02
SMTP	0,003	0,006	0,012	0,025	0,038
DNS	0,005	0,01	0,027	0,033	0,095
HTTP	0,011	0,019	0,033	0,07	0,119

На рис.3.25. показаний графік залежності джитеру від загальної швидкості генерації трафіку для чотирьох типів трафіку, які використовуються в експерименті.

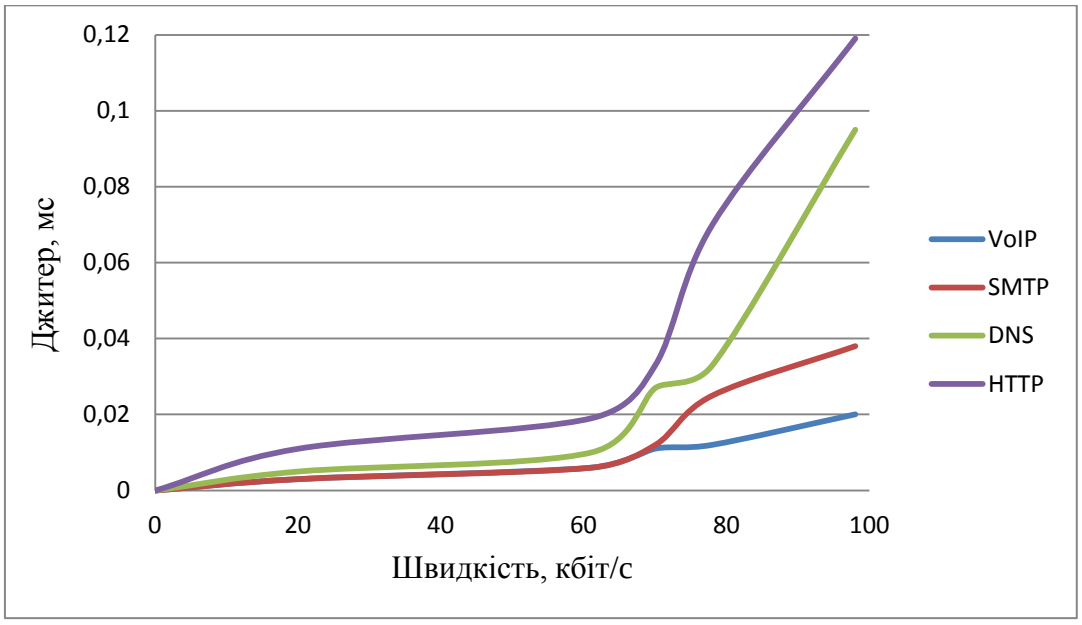


Рисунок 3.25 Графік залежності варіативності для чотирьох типів трафіку від загальної швидкості генерації мережевого трафіку (CQ)

3.3 Порівняльний аналіз результатів експериментів стосовно VoIP-трафіку

Порівняльна таблиця 3.15. за показником втрата пакетів IP-телефонії для технологій управління мережевим трафіком FIFO, CQ та PQ.

Табл. 3.15 Порівняння таблиця за показником втрата пакетів

Тип трафіку	Втрата пакетів, %				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
FIFO	0	11,12	26,71	38,33	46,33
CQ	0	0	0	0	1,6
PQ	0	0	0	0	0

На рис.3.26. зображений порівняльний графік за показником залежності втрати пакетів IP-телефонії від загально об’єму мережевого трафіку.

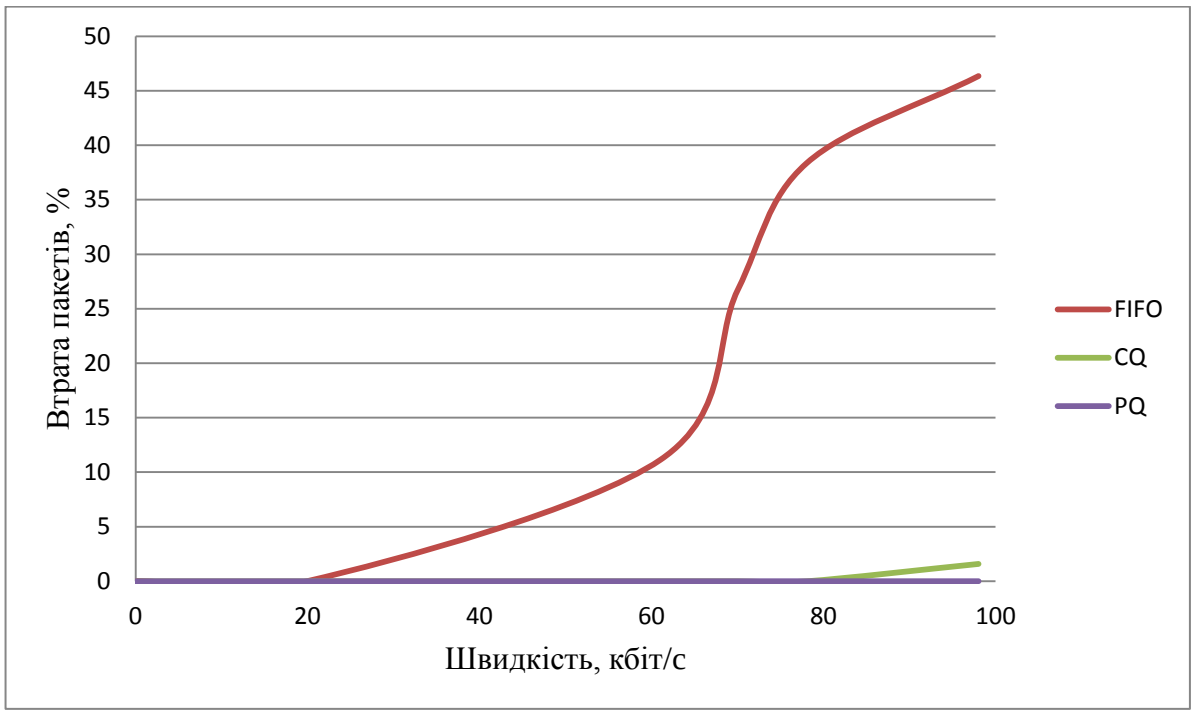


Рисунок 3.26 Порівняльний графік за показником втрата пакетів

Проаналізувавши показники втрати пакетів та порівняльний графік залежності втрати пакетів IP-телефонії від загальної швидкості генерації мережевого трафіку , ми дійшли до висновку, що при всіх різновидах навантажень на мережу, для підвищення якості IP-телефонії краще підходить технологія управління мережеви трафіком PQ.

Порівняльна таблиця 3.16. за показником бітрейт IP-телефонії для технологій управління мережевим трафіком FIFO, PQ.CQ.

На рис.3.27. зображений порівняльний графік за показником залежності біт рейту IP-телефонії від загально об’єму мережевого трафіку.

Табл. 3.16 Порівняння таблиця за показником бітрейт

Тип трафіку	Бітрейт, кбіт/с				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
FIFO	5,1	14,3	14,5	15,5	12,5
CQ	5,1	15,2	17,5	19,2	23,1
PQ	5,2	15,4	17,4	19,5	24,6

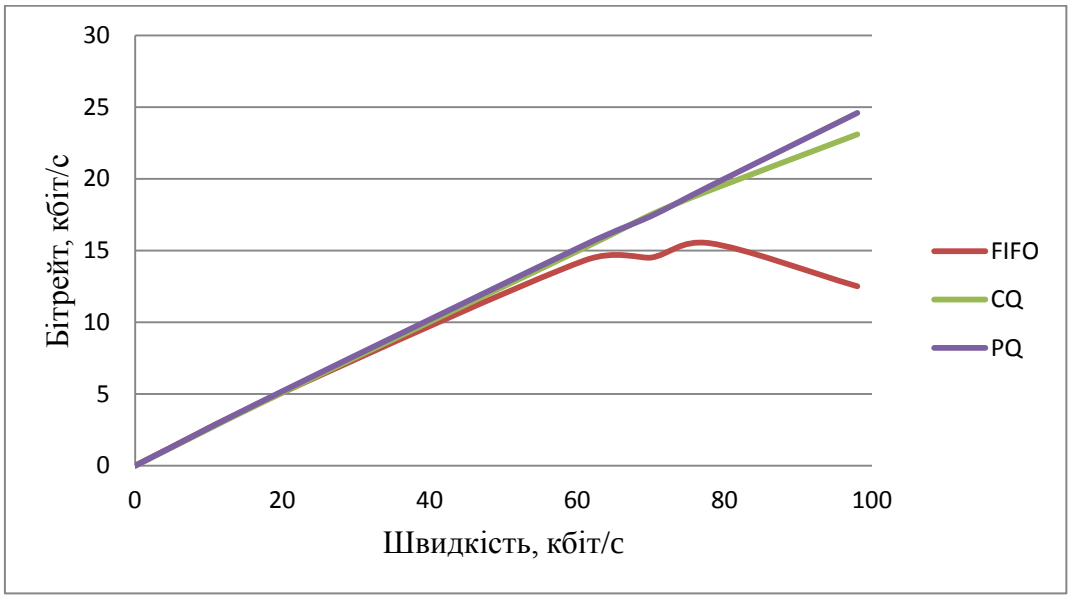


Рисунок 3.27 Порівняльний графік за показником бітрейт

Проаналізувавши показники бітрейту та порівняльний графік залежності бітрейту IP-телефонії від загальної швидкості генерації мережевого трафіку , ми дійшли до висновку, що при всіх різновидах навантажень на мережу, для підвищення якості IP-телефонії краще підходить технологія управління мережеви трафіком PQ. Порівняльна таблиця 3.17. за показником затримка пакетів IP-телефонії для технологій управління мережевим трафіком FIFO, PQ.CQ.

Таблиця 3.17 Порівняння таблиця за показником затримка пакетів

Тип трафіку	Середня затримка, мс				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
FIFO	2,24	3,16	8,41	12,63	19,4
CQ	2,2	2,23	2,27	2,33	2,41
PQ	2,21	2,23	2,36	2,4	2,48

На рис.3.28. зображений порівняльний графік за показником залежності затримки пакетів IP-телефонії від загально об’єму мережевого трафіку.

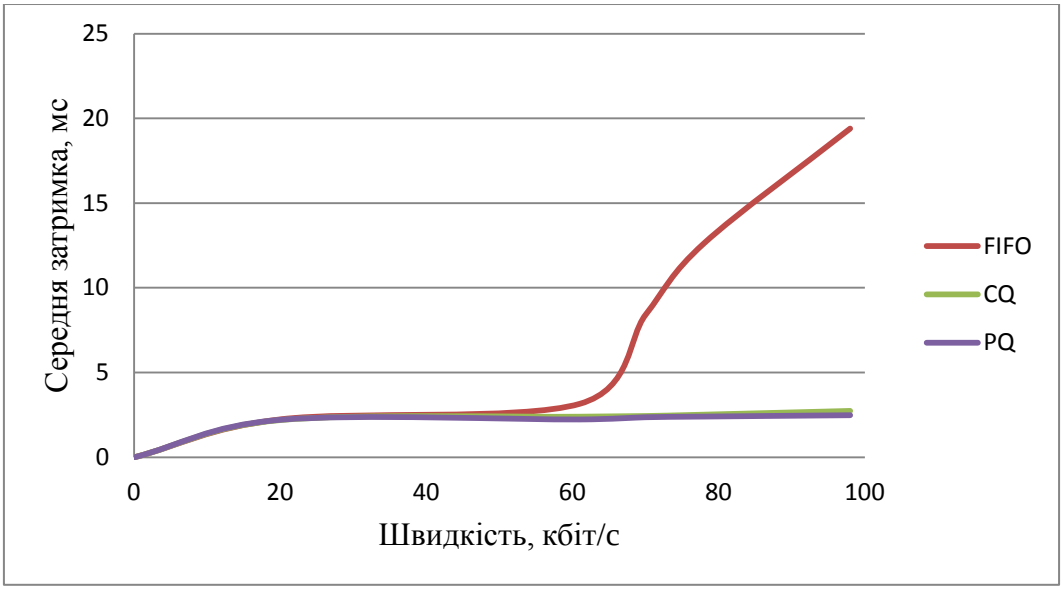


Рисунок 3.28 Порівняльний графік за показником затримка пакетів

Проаналізувавши показники затримки пакетів та порівняльний графік затримки пакетів IP-телефонії від загальної швидкості генерації мережевого трафіку, ми дійшли до висновку, що при всіх різновидах навантажень на мережу, для підвищення якості IP-телефонії краще підходить технологія управління мережеви трафіком PQ.

Порівняльна таблиця 3.18 за показником варіативність трафіку IP-телефонії для технологій управління мережевим трафіком FIFO, PQ.CQ.

На рис.3.29. зображений порівняльний графік за показником залежності варіативності трафіку IP-телефонії від загально об’єму мережевого трафіку.

Таблиця 3.18 Порівняння таблиця за показником джитер

Тип трафіку	Джитер, мс				
	№1 (20кбіт/с)	№2 (61кбіт/с)	№3 (70кбіт/с)	№4 (78кбіт/с)	№5 (98кбіт/с)
FIFO	0,009	0,016	0,025	0,037	0,068
CQ	0,003	0,007	0,011	0,012	0,02
PQ	0,003	0,006	0,011	0,011	0,01

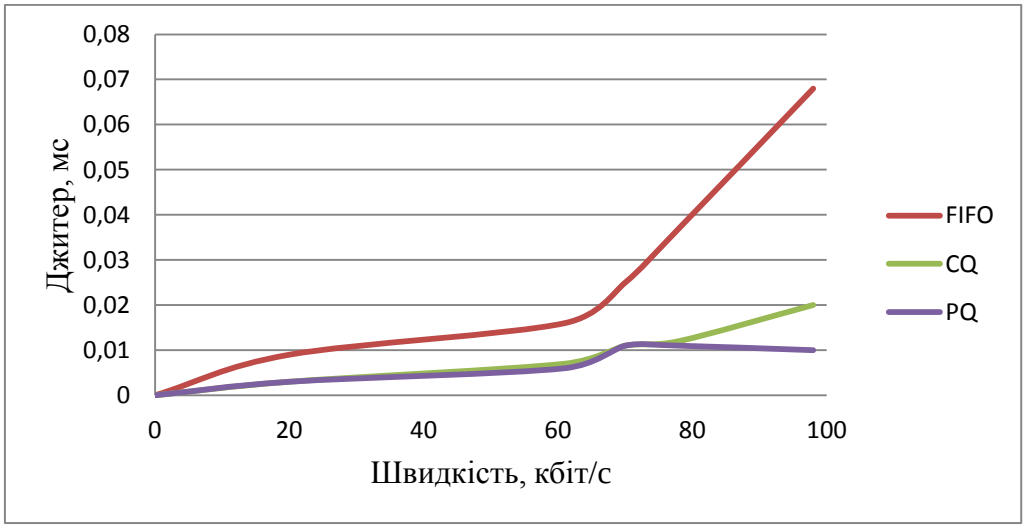


Рисунок 3.29 Порівняльний графік за показником джитер

Проаналізувавши показники затримки пакетів та порівняльний графік затримки пакетів IP-телефонії від загальної швидкості генерації мережевого трафіку, ми дійшли до висновку, що при всіх різновидах навантажень на

мережу, для підвищення якості IP-телефонії краще підходить технологія управління мережеви трафіком PQ.

3. 4 Висновки до розділу 3

Провівши експериментальне дослідження і порівнявши три технології управлянні мережевим трафіком FIFO, PQ та CQ, можна зробити висновок проаналізувавши отримане:

Коли загальний об’єм мережевого трафіку значно нижчий за пропускну здатність(64кбіт/с), то всі технології показують майже один і той же результат - тобто невеликі затримки і джитер, однакомий бітрейт, відсутність втрат пакетів.

Коли загальний об’єм мережевого трафіку наближається до пропускної здатності, то що можна використовувати як технологію CQ так і PQ для підвищення якості IP-телефонії (їх показники приблизно однакові), по-друге, показники технології FIFO значно гірші - середня затримка пакетів при передачі високопріорітетного трафіку вища у 1.5 рази (див. таблицю 3.17), тому для задач поставлених перед нами не підходить.

Коли загальний об’єм мережевого трафіку значно вище за пропускну здатність, то показники технології управляння мережним трафіком PQ, щадо втрат і затримки, вищі ніж у технологій CQ та FIFO, хоча таку поведіку можна побачити вже при перевищенні загальної генерації трафіку 90кбіт/с, тобто у 1.5 рази. Технологія управляння мережним трафіком PQ краще підходить для вирішення задачі управління і забезпечення якості передачі високопріорітетного трафіку в умовах перевантаженної мережі.

Технологія управління мережевим трафіком PQ найкраще підходить, як інструмент пріорітизації мережевого трафіку для підвищення якості IP-телефонії.

ВИСНОВКИ

Проаналізовано методи для підвищення в QoS мультисервісних IP-мережах. Детально розглянуто характеристики, які впливають на якість обслуговування в розрізі мережевої моделі взаємодії відкритих систем. Особливу увагу звернено на такий високопріорітетний трафік як VoIP.

Побудована метематична модель TCP-сеансів з урахуванням AQM-алгоритмів. Для аналізу стійкості був вибраний математичний апарат теорії біфуркацій, оскільки він грунтується на моделях, що описуються диференціальними рівняннями, і не вимагає необхідності побудови специфічних функцій, як у випадках застосування методів Ляпунова і теорії катастроф. В рамках даної теорії забезпечується безпосередній облік параметрів і змінних на рівні математичного опису вихідної динамічної моделі.

Запропоновано варіант реалізації політик QoS мультисервісних IP-мережах. Досліджені параметри, такі як втрата пакетів, затримка, бітрейт та джитер при передачі чотирьох потоків VoIP, SMTP, DNS, HTTP. Найвищий пріорітет надавався VoIP, високий - SMTP, середній - DNS і низький - HTTP. Проведено аналіз поведінки високопріорітетного трафіку VoIP щодо FIFO, PQ, CQ технологій управління чергами. При наявності IP-телефонії у мережі краще з розглянутого буде реалізація політик PQ.

Основні положення і результати дисертаційної роботи знайшли своє відображення у 3 публікаціях: на Дванадцятій міжнародній науково-технічній конференції "Проблеми телекомунікацій", 2018 р. (ІТС, НТУУ “КПІ ім. Ігоря Сікорського”), Одинадцята міжнародна науково-технічна конференція "Проблеми телекомунікацій", 2017 р. (ІТС, НТУУ “КПІ ім. Ігоря Сікорського”) та на Міжнародній науково-практичній конференції «Проблеми інфокомунікацій », 2016.

ПЕРЕЛІК ПОСИЛАНЬ

1. Мєлєхова М. О. Аналіз Аналіз алгоритмів регулювання завантаженості IP-мережі../ М.О. Мєлєхова, В.І. Носков, К.В. Герасименко, О.В. Старкова // Одинадцята міжнародна науково-технічна конференція \"Проблеми телекомунікацій\", 2017. – с. 149-152.
2. IP-сети - Стандарты_QoS [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://ru.bmstu.wiki/IP-сети_-_Стандарты_QoS/.(01.05.2018)
3. Таненбаум Э. Компьютерные сети. Принципы технологии, протоколы: учебник для студ. высш. уч. зав. / Э. Таненбаум, Д. Уэзеролл. – [5-е изд.]. – СПб.: Питер, 2012. – 964с.
4. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCETN/CCNA ICND1 640-822 / Третье издание , 2013 - 720 с.
5. Олифер В. Г. Компьютерные сети. Принципы технологии, протоколы: учебник для студ. высш. уч. зав. / В. Г. Олифер, Н. А. Олифер. – [5-е изд.]. – СПб.: Питер, 2016. – 996с.
6. General Recommendations on the transmission quality for an entire international telephone connection // ITU-T Recommendation G.114. – 2003.
7. Network Performance objectives for IP-based services // ITU-T Recommendation Y.1540/Y.1541. – 2006.
8. Олифер В. Искусство оптимизации трафика / Олифер В, Олифер Н.. // Журнал сетевых решений. – 2001. – с. 38–47.
9. Уровни эталонной модели OSI. Технологии MIMO и mesh-сети. [Електронний ресурс] – Режим доступу до ресурсу: http://www.incore.me/internet-texnologii/urovnej-etalonnoj-modeli-osi-texnologii-mimo-i-mesh-seti/.(01.05.2018)
10. Как различать и считать маркированный трафик? [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: http://samag.ru/archive/article/306/.(01.05.2018)

11. TCP three-way handshake [Електронний ресурс] – Режим доступу до ресурсу: httPs://www.pinterest.com/pin/377035800030574666/.(01.05.2018)
12. Основы IP-телефонии, базовые принципы, термины и протоколы [Електронний ресурс] / Habr. – 2013. – Режим доступу до ресурсу: https://habr.com/post/183152/. (01.05.2018)
13. Еталонна модель взаємодії відкритих систем. Електронний ресурс] – Режим доступу до ресурсу: https://studfiles.net/preview/5199491/page:2//. (01.05.2018)
14. Вегешна Ш. Качество обслуживания в сетях IP / Ш. Вегешна, 2003. – 368 с.
15. Битнер В. И. Сети следующего поколения [Електронний ресурс] / В. И. Битнер. – 2008. – Режим доступу до ресурсу: httPs://studfiles.net/preview/3515833/Page:13/.(01.05.2018)
16. Мєлєхова М. О. Інтернет речей в сучасних телекомунікаційних мережах / М.О. Мєлєхова, А.М. Білан // Восьма міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» /, 2016. – с. 568-569.
17. OSPF Version 2// IETF Recommendation 2178. – 1998.
18. Маршрутизація [Електронний ресурс] // – Режим доступу до ресурсу: httPs://www.wikiplanet.click/enciclopedia/uk/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F/. (01.05.2018)
19. Chitra K. Classification and Performance of AQM-Based Schemes for Congestion Avoidance / K. Chitra, D. Padamavathi. // 8. – 2010. – №1. – с. 331–340..
20. Ali Ahammed. Analyzing the Performance of Active Queue Management Algorithms / Ali Ahammed, B. Reshma. // International journal of Computer Networks & Communications (IJCNC).. – 2010. – №2. – с. 36–55..
21. Cisco QoS – классификация и маркировка [Електронний ресурс] // Twistedminds – 2016. – Режим доступу до ресурсу: http://twistedminds.ru/2013/02/cisco-qos-classifying-and-marking/. (01.05.2018)

22. Мєлєхова М. О. Забезпечення QoS в TCP/IP мережах / М.О. Мєлєхова, В.І. Носков // Дванадцята міжнародна науково-технічна конференція \"Проблеми телекомунікацій\" , 2018. – С. 137-139.
23. Старкова Е.В. Анализ устойчивости и оптимизация TCP–сеансов в мультисервисных ТКС [Електронний ресурс] / Е.В. Старкова // Проблеми телекомунікацій. – 2010. – № 1 (1). – С. 45 – 58. – Режим доступу до журн.: http://pt.journal.kh.ua/2010/1/1/101_starkova_stability.pdf. (01.05.2018)
24. Lemeshko. A flow-based model of dynamic queue balancing in the MPLS-network with Traffic Engineering Queues support / Lemeshko, Ali, Starkova. // CAD Systems in Microelectronics (CADSM). – 2011. – с. 116–117.
25. Лемешко А. Мультитензорная интерпретация решения маршрутных задач в телекоммуникационных сетях, представленных мнопродуктовыми многополюсными моделями евклидового пространства / А. В. Лемешко // Радіоелектронні і комп'ютерні системи. - 2003. - № 3. - с. 115–126. - Режим доступу: http://nbuv.gov.ua/UJRN/recs_2003_3_24 (01.05.2018)
26. D-ITG 2.8.1 Manual [Електронний ресурс] // – Режим доступу: http://traffic.comics.unina.it/software/ITG/manual/ (01.05.2018).
27. Подходы к представлению результатов анализа сетевого трафика / [А. Гетьман, Ю. Маркин, Д. Обыденков та ін.]. // Труды Института системного программирования. – 2016. – №28. – с. 103–154.
28. WAN and Application Optimization Solution Guide [Електронний ресурс] / Cisco – 2008. – Режим доступу до ресурсу: https://www.cisco.com/c/en /us/td/docs/nsite/enterprise/wan/wan_optimization/wan_opt_sg.pdf/. (01.05.2018)
29. Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: httPs://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfconmg.html/.(01.05.2018)
30. Качество обслуживания в операторских сетях [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.opennet.ru/docs/RUS/qos_oper/ (01.05.2018)

31. Mieliekhova M. Prioritization of Network Traffic to Improve VoIP Traffic Quality / M. Mieliekhova, O. Starkova, K. Herasymenko. // Third International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2016). – 2016.